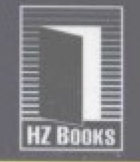
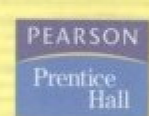
华章数学译丛

40





Algebra

代数

(美) Michael Artin 著
麻省理工学院

郭晋云 译

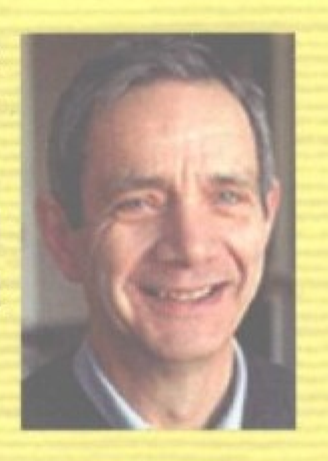
机械工业出版社
China Machine Press

代数

本书由著名代数学家与代数几何学家Michael Artin所著，是作者在代数领域数十年的智慧和经验的结晶。书中既介绍了矩阵运算、群、向量空间、线性变换、对称等较为基本的内容，又介绍了环、模、域、伽罗瓦理论等较为高深的内容，本书对于提高数学理解能力、增强对代数的兴趣是非常有益处的。此外，本书的可阅读性强，书中的习题也很有针对性，能让读者很快地掌握分析和思考的方法。

本书在麻省理工学院、普林斯顿大学、哥伦比亚大学等著名学府得到了广泛采用，是代数学的经典教材之一。

作者简介



Michael Artin 当代领袖型代数学家与代数几何学家之一，美国麻省理工学院教授。由于他在交换代数与非交换代数、环论以及现代代数几何学等方面做出的毕生贡献，2002年获得美国数学学会颁发的Leroy P. Steele终身成就奖。Artin的主要贡献包括他的逼近定理、在解决沙法列维奇–泰特猜测中的工作以及为推广"概形"而创建的"代数空间"概念。

Algebra

影印版

ISBN 7-111-13913-5

定价：59.00元

www.pearsonhighered.com

投稿热线：(010) 88379604

购书热线：(010) 68995259, 68995264

读者信箱：hzjsj@hzbook.com

华章网站 http://www.hzbook.com

网上购书：www.china-pub.com

封面设计·杨宇梅

上架指导：数学

定价：69.00 元

华章数学译丛 40

Algebra

代数

（美）Michael Artin 麻省理工学院 著
郭晋云 译

机械工业出版社
China Machine Press

本书是一本代数学的经典著作，既介绍了矩阵运算、群、向量空间、线性变换、对称等较为基本的内容，又介绍了环、模、域、伽罗瓦理论等较为高深的内容，对于提高数学理解能力、增强对代数的兴趣是非常有益处的.

本书是一本有深度、有特点的著作，适合数学工作者以及基础数学、应用数学等专业的学生阅读.

本书版权登记号：图字：01-2005-0899

图书在版编目(CIP)数据

代数/(美)阿廷(Artin, M.)著；郭晋云译．—北京：机械工业出版社，2009.1

(华章数学译丛)

书名原文：Algebra

ISBN 978-7-111-25356-3

Ⅰ.代…　Ⅱ.①阿…　②郭…　Ⅲ.代数　Ⅳ.O15

中国版本图书馆 CIP 数据核字(2008)第 161443 号

机械工业出版社(北京市西城区百万庄大街 22 号　邮政编码　100037)

责任编辑：迟振春

北京瑞德印刷有限公司印刷·新华书店北京发行所发行

2009 年 1 月第 1 版第 1 次印刷

186mm×240mm·30.5 印张

标准书号：ISBN 978-7-111-25356-3

定价：69.00 元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：(010)68326294

译者序

美国数学学会在2002年授予Michael Artin教授Steele终身成就奖时，在评价中有这样一段话："许多年来他的代数课程是麻省理工学院教育的一个特色，现在全世界都可以通过他的教科书分享其中的一些见解."本书就是这本教科书的中译本.

这是一本很有特色的代数书. 自1965年Serge Lang的《Algebra》以来，本科生和研究生层次的代数教材出了不少，但内容和架构不出Serge Lang书的范围. 这并不是说那些书都不好，而是Serge Lang的代数书确实是一个经典. Serge Lang的书以培养抽象化思维能力为基点，书中的内容大多从纯粹抽象代数的观点出发，结合数论中的一些方法，尽管把抽象代数的内容进行了统一的抽象处理，但并没有把代数同其他数学分支广泛联系起来. Michael Artin所著的这本书脱开了Serge Lang的桎梏. 作为一个代数几何学家(偏向代数的背景)，他在本书中尽力强调代数同其他数学分支的联系，尤其是同拓扑以及代数几何的联系，书中的很多章节都对抽象的概念进行了直观的解释或者给出了形象的例子，使读者能看到一个个用抽象定义的概念背后的图形，并体会到代数在其他分支中的威力和另一种风格的数学美.

对于希望以后攻读代数的学生，这本书能开阔他们的视野. 对于其他分支的学生，这本书中的代数知识是成为一个数学家所必须具备的基础知识.

历时1年译完这本原著近600页的书后，我有两点遗憾，一是我没能在25年之前看到这本书，二是只有1年的时间来进行翻译. 25年前是我上大学的时候，假如那时我读了这本书，应该会有更高的数学品位，对数学特别是对代数及其意义会有一个更为全面和深入的认识，避免一些走过的弯路. 1年的时间实在太短，但愿我粗拙的汉语表达不致影响你对大师数学思想之美的欣赏.

前言

虽然时新的和孜孜以求追求公理化和一般化的激情，
带给我们的一般概念和命题可能是重要的，
而且这在代数学中也许胜于任何其他领域，
但是我坚信，各种特殊的问题以其极端的复杂性构成数学的基干和核心，
而掌握其难点从整体上需要更刻苦地工作．

Herman Weyl

本书源于大约20年前我的代数课补充讲义．我那时想比教材中更为详细地讨论如对称、线性群和四元数域等具体内容，而将群论的重点由置换群转到矩阵群．格——另一个常见的主题，让它很自然地出现．我的希望是具体的东西会使学生感兴趣且会使抽象更易理解，简言之，他们可同时学习二者而学得更深．这项工作进行得很顺利．我花了很长时间来确定加上些什么，我逐渐写出了更多的讲义而最终仅用讲义而不用其他教材．这种办法形成了一本我认为与已有的书都有所不同的书．然而，当我把材料汇总起来时遇到了不少头疼的事，因而我不推荐以这样的方式开始写书．

本书最突出的特点是加大对特殊主题的强调．每次重写这些章节时，它们都在膨胀．因为多年来我注意到，与抽象概念不同，学生对于具体的数学题材是多多益善．结果，上面提到的这些东西成了本书的主体．另外，书中也有一些不常见的主题，如托德-考克斯特算法和 PSL_2 的单性．

在写本书时，我尽力遵循下面的原则：

1. 主要例子应放在抽象定义之前．

2. 本书不是作为一本"服务教程"(手册、指南或诸如此类的书)，因此技巧只应在用到的时候提及．

3. 所有讨论的主题对于一般的数学工作者而言都应是重要的．

虽然这些原则听起来像是写书的本源和路标，但我发现把它们讲出来是很有用的，要记住，"按你所教的写"并不在这些原则之中．当然，我有时也会违反这些原则．

目录给出了本书主题内容的很好的线索，不过乍一看会使你认为本书包含了代数入门课程的所有标准材料或者更多．但更仔细看一看，你会发现不时会有一些东西被省去而让位给特别的主题．上面的原则是我的指南．在进入抽象内容之前给出主要例子，使得一些抽象能被处理得更简洁．在学生克服固有的概念性困难以后再进行某些讨论，还使我压缩了一些东西．如第十章佩亚诺公理的讨论，就被减到两页[⊖]．虽然其讨论是相当不完整的，但我的经验是这已经

⊖ 这是指原英文书．——编辑注

足以使学生体会到整数算术公理化的发展. 如果把它放到书的前面，就需要进行更为广泛的讨论，为此而花费时间是不值得的. 有时推后的内容可以一直推下去，那不是本质的. 例如，对偶空间和多线性代数，根据第二条原则被搁置起来. 对于一些概念，比如极小多项式，我最终认为将它们包括进入门性代数书中的主要目的是提供方便的练习来源.

本书各章按照我通常教课的顺序安排. 线性代数、群论和几何构成第一学期的内容. 环在第十章才引入，虽然该章在逻辑上独立于前面许多章节. 我采用这种非常规安排的原因是我想从一开始就强调代数与几何的联系，而且也是因为前面几章的内容对其他领域的人来说毕竟是最重要的. 缺点是计算受到忽视. 后面几章中向计算的倾斜，是对此的补偿. 在后面的几章里，几何又以格、对称和代数几何的面貌多次出现.

Michael Artin

1990 年 12 月

给教师的话

本书需一些预备知识. 学生应熟悉微积分、复数的基本性质和数学归纳法. 了解证明肯定是有用的，但不是必不可少的. 第八章用到的拓扑学概念并不作为预备知识要求，附录介绍了这些概念，但太简短，不宜作教材.

不要试图在一学年讲完本书，除非你的学生已学过一学期的代数课程(如线性代数)，而且数学上相当成熟. 大约三分之一的内容可略去(而不影响连贯性)，如果需要，还可省去更多. 下列章节可以构成一门连贯的课程：

第一章，第二章，第三章的第一节～第四节，第四章，第五章的第一节～第七节，第六章的第一节和第二节，第七章的第一节～第六节，第八章的第一节～第三节和第五节，第十章的第一节～第七节，第十一章的第一节～第八节，第十二章的第一节～第七节，第十三章的第一节～第六节.

这一选择包括一些有意义的特殊主题：平面图形的对称，SU_2 的几何，虚二次数域的算术. 如果你不想讨论这些主题，那么这本书不适合你.

用一个学期来学前面四章是容易的，但这样将偏离本书的目标. 因为真正有意义的内容从第五章开始，坚持下去很重要. 如果你计划逐章学习，可以保持轻松的节奏尽可能快地进入第五章. 把注意力放在具体例子上会很有帮助，这对于一开始对证明的构成没有明确概念的学生而言是特别重要的.

与后面几章相比，第一章不那么吸引人，因此应快速讲完. 本书以它开始的原因是我想从一开始就强调一般线性群，而不是按通常做法将例子基于对称群. 这个决定的根据是前言中的第三条原则：一般线性群更重要.

下面是关于第二章的一些建议：

1. 对抽象的材料浅尝辄止，你在第五、六章还会遇到它们.

2. 例如，注重矩阵群，置换群只是一带而过. 由于其固有的记号上的困难，对称的例子(比如二面体群)最好推迟到第五章讲授.

3. 不要在算术上花太多时间，本书中其自然的位置是第十、十一章.

4. 不强调商群构造.

商群在教学上有问题. 虽然其构造在概念上很难，但在大多数初等例子中，商群很容易表示为同态的象，因而不需要抽象定义. 模算术几乎是其仅有的反例. 但模 n 的整数构成一个环，对于群的商，模算术不是理想的具有启发性的例子. 第一次真正使用商群是在第六章讨论生成元和关系时，本书早期手稿中，我曾把商群放在那里介绍. 由于担心引起代数界的不满，我最后把它放到第二章. 总之，如果你不打算在课程中讲授生成元与关系，那么可将商的深入讨论推迟到第十章(环论)，它在那里起着至关重要的作用，而且在那里模算术成为了极佳的具

有启发性的例子.

在第三章(向量空间)中，我试图建立这样一种用基计算的方式，它使学生不会为保持下标一致而产生麻烦. 我也许并不成功，但全书都使用该记号，建议最好采用.

因为后面要用到，所以第四章关于线性算子在旋转和线性微分方程组的应用应加以讨论，但不要陷入过多讲授微分方程的诱惑. 因为你在教代数课程，这种信念应被原谅.

在前面几章里，复杂程度逐渐增加，但第五章的内容有些跳跃. 如果不是有这个跳跃，我会尽可能把对称群放在前面讲述. 记住对称是一个困难的概念.

除了前两节，第六章的内容是可选的. 最后一节关于托德-考克斯特算法的内容不是标准的，把它放进来是用于为生成元和关系的讨论提供实例，否则没什么用.

关于双线性型的第七章没有什么特别的. 我没能解决这部分内容的主要问题，即对同一主题有太多的变化，但通过集中于实的和复的情形，我试图使讨论尽量简短.

在关于线性群的第八章，计划把时间花在 SU_2 的几何上. 在我扩充关于 SU_2 一节之前，我的学生每年都抱怨，之后他们开始要求补充读物，想学更多的东西. 许多学生在上这门课时不熟悉拓扑概念，因而这些概念需要过一下. 但我发现学生不熟悉拓扑概念所带来的困难是可以克服的. 的确，这里是他们学习流形是什么的好地方. 可是，我不知道有什么可以作为继续阅读的令人满意的参考文献.

关于群表示的第九章是可选的. 若干年来我一直反对包括这一主题，因为它太难了. 但学生常常要求学习这一主题，我也一直问自己：如果化学家能教，我们为什么不能呢？最终，根据本书的结构要求，还是纳入了群表示这一主题. 正由于此，埃尔米特型有了一个应用.

第十一章中非同寻常的主题是二次数域的算术. 你会发现，对于一般的代数课程来说，其讨论太长. 基于这种考虑，我将第八节(理想因子分解)作为一个自然的结束点.

在入门级的代数课程中，似乎应提及域的最重要的例子，因此第十三章讨论了有关函数域的内容.

伽罗瓦理论是否应放到本科课程中一直是一个有争议的问题. 虽然它的应用没有本书其他大部分主题那样广泛，但由于伽罗瓦理论是对称讨论的高潮，故把它作为一个可选主题. 我通常至少会花一些时间在第十四章上.

我曾考虑将练习根据其难度分级，但我发现无法保持一致，因而只在一些较难的题上用星号标记. 我相信已有足够多的难题，但当然我们总需要有更多有意义、容易的题目.

虽然我教了多年代数，但本书的若干方面仍是实验性的，我非常感谢使用本书的人提出的批评和建议.

“一、二、三、五、四……”

“不！爸爸，是一、二、三、四、五.”

“哎，如果我想说一、二、三、五、四，为什么不行呢？”

“不是那样数数的.”

致 谢

我主要想感谢多年来上我课的学生，他们使得这门课程令人激动. 请原谅这里没有单独提到其中许多人的名字.

不少人在课堂上用过我的讲义并提出了有价值的建议，其中有 Jay Goldman、Steve Kleiman、Richard Schafer 及 Joe Silverman. Harold Stark 在数论方面以及 Gil Strang 在线性代数方面向我提供了帮助. 此外，下列诸位阅读并评论了本书的手稿：Ellen Kirkman、Al Levine、Barbara Peskin 及 John Tate. 我特别要感谢 Barbara Peskin 在生命的最后一年还把整本书读了两遍.

书中精确的数学图是 George Fann 和 Bill Schelter 利用计算机制作的. 凭我一己之力无法完成.

感谢 Marge Zabierek，大约八年她每年都重录一次手稿，这样我才能在计算机上进行修改，还要感谢 Mary Roybal 对手稿进行仔细和专业的加工.

我在写本书时对其他书参考得不多，但伯克霍夫和麦克莱恩的经典著作以及师从范德瓦尔登的学习对我影响很大. Herstein 的书也一样，我曾多年用之作为教材. 在 Noble 的书以及 Paley 和 Weichsel 的书中我发现一些关于练习的好的想法.

一些引文(大都与内容无关)散布于书中. 我从阿诺尔德(V. I. Arnold)处得知第五章和第六章结束处的莱布尼茨和罗素的引文，从克莱因(Morris Klein)的《Mathematical Thought from Ancient to Modern Times》(古今数学思想)一书中看到第八章开始处外尔(Weyl)的引文.

目　录

第一章 矩阵运算

有了一些增加或减少，
或在上面添加一点或拿走一点，
人们在第一眼还是会说大小没变.

Leonhard Euler

矩阵是本书中心角色. 它是理论的重要组成部分，并且许多具体例子都基于矩阵. 因而，发展处理矩阵的方法是非常重要的. 因为矩阵遍及大部分数学学科，所以这里用到的技巧在其他地方也一定会有用.

需要通过实践掌握的概念有矩阵乘法和行列式.

第一节 基本运算

设 m，n 为正整数. 一个 $m\times n$ 矩阵是按矩形阵列排列的 mn 个数：

【1.1】
$$m\text{行}\overset{n\text{列}}{\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}}.$$

例如，$\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix}$是 2×3 矩阵.

矩阵中的数称为矩阵元素，用 a_{ij} 表示，其中 i，j 为指标(整数)，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$. 指标 i 称为行指标，而 j 称为列指标. 因而 a_{ij} 是位于矩阵 i 行 j 列的元素：

$$i\overset{j}{\begin{bmatrix} & \vdots & \\ \cdots & a_{ij} & \cdots \\ & \vdots & \end{bmatrix}}.$$

在上面的例子中，$a_{11}=2$，$a_{13}=0$，而 $a_{23}=5$.

我们通常用记号 A 表示矩阵，或者也可以把它写作(a_{ij}).

$1\times n$ 矩阵称为 n 维行向量. 当 $m=1$ 时我们去掉指标 i 而将行向量写作

【1.2】
$$A=[a_1 \cdots a_n] \quad \text{或} \quad A=(a_1,\cdots,a_n).$$

行向量中的逗号可有可无. 类似地，$m\times 1$ 矩阵是 m 维列向量：

【1.3】
$$B=\begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}.$$

1×1 矩阵$[a]$仅含有一个数，我们不区分这样的矩阵和它的元素.

【1.4】矩阵的加法是向量相加：

$$(a_{ij})+(b_{ij})=(s_{ij}),$$

其中对所有 i，j，有 $a_{ij}+b_{ij}=s_{ij}$. 这样

$$\begin{bmatrix}2 & 1 & 0\\1 & 3 & 5\end{bmatrix}+\begin{bmatrix}1 & 0 & 3\\4 & -3 & 1\end{bmatrix}=\begin{bmatrix}3 & 1 & 3\\5 & 0 & 6\end{bmatrix}.$$

只有当两个矩阵 A，B 具有相同的形状，即它们都是 $m\times n$ 矩阵时，才能定义它们的和.

【1.5】矩阵与数的标量乘法定义与向量的标量乘法一样. 数 c 与矩阵(a_{ij})相乘的结果是另一个矩阵：

$$c(a_{ij})=(b_{ij}),$$

其中对所有 i，j，有 $b_{ij}=ca_{ij}$. 于是

$$2\begin{bmatrix}0 & 1\\2 & 3\\2 & 1\end{bmatrix}=\begin{bmatrix}0 & 2\\4 & 6\\4 & 2\end{bmatrix}.$$

2 数也称为标量.

矩阵乘法是一个复杂的概念. 我们先学习同样大小(即 $m=n$)的一个行向量 A(上面的(1.2))和一个列向量 B(上面的(1.3))的积 AB. AB 是 1×1 矩阵，即标量

【1.6】
$$a_1b_1+a_2b_2+\cdots+a_mb_m.$$

(这个积通常叫做这两个向量的“点积”.)这样

$$\begin{bmatrix}3 & 1 & 2\end{bmatrix}\begin{bmatrix}1\\-1\\4\end{bmatrix}=3\cdot 1+1\cdot(-1)+2\cdot 4=10.$$

当我们把 A，B 看成带有下标的量时，这个定义的作用是很明显的. 例如，考虑含有 m 种成分的糖果条，用 a_i 表示每一糖果条中(成分)$_i$ 的克数，b_i 表示每克(成分)$_i$ 的价格，则矩阵乘积 $AB=C$算出每个糖果条的价格：

$$(\text{克}/\text{条})\cdot(\text{价格}/\text{克})=(\text{价格}/\text{条}).$$

另一方面，这是任意选择的行列乘积的定义.

一般地，对于两个矩阵 A 与 B，只有当 A 的列数等于 B 的行数时它们的积才有定义. 比如说，A 是一个 $\ell\times m$ 矩阵，而 B 是一个 $m\times n$ 矩阵. 这时积是一个 $\ell\times n$ 矩阵. 从符号上看，有$(\ell\times m)\cdot(m\times n)=(\ell\times n)$. 利用上面(1.6)的规则，积矩阵的元素通过将 A 的每一行与 B 的每一列相乘得到. 因此，若用 P 表示积 AB，则

【1.7】
$$p_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots+a_{im}b_{mj}.$$

下面是 A 的第 i 行与 B 的第 j 列的积.

$$i \boxed{a_{i1} \cdots a_{im}} \cdot \begin{array}{c} j \\ \boxed{\begin{matrix} b_{1j} \\ \vdots \\ b_{mj} \end{matrix}} \end{array} = \boxed{\begin{matrix} & \vdots & \\ \cdots & p_{ij} & \cdots \\ & \vdots & \end{matrix}}$$

例如，

【1.8】

$$\begin{bmatrix} 0 & -1 & 2 \\ 3 & 4 & -6 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

矩阵乘法的这种定义方法提供了非常方便的计算工具.

回到糖果条例子，设有 ℓ 种糖果条，则可构造一个矩阵 A，使其第 i 行给出(条)$_i$ 的各成分的克数. 如果要算 n 年中每一年的价格，则可以构造一个矩阵 B，使其第 j 列是(年)$_j$ 的各成分的价格值. 矩阵乘积 $AB=P$ 算出糖果条的价格：$p_{ij}=$(条)$_i$ 在(年)$_j$ 的价格.

矩阵的概念是 19 世纪为了提供一个书写线性方程组的简明形式而引入的. 线性方程组

$$\begin{matrix} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ & & & & & & & \vdots & \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \cdots & + & a_{mn}x_n & = & b_m \end{matrix}$$

可利用矩阵记号写为

【1.9】

$$AX = B,$$

其中 A 为系数矩阵(a_{ij})，X 和 B 为列向量，而 AX 为矩阵乘积

$$\boxed{\quad A \quad} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}.$$

这样矩阵方程

$$\begin{bmatrix} 0 & -1 & 2 \\ 3 & 4 & -6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

表示如下的三个未知量的线性方程组：

$$\begin{matrix} & & -x_2 & + & 2x_3 & = & 2 \\ 3x_1 & + & 4x_2 & - & 6x_3 & = & 1. \end{matrix}$$

方程(1.8)给出其一个解：$x_1=1$，$x_2=4$，$x_3=3$.

公式(1.7)定义的积也可用求和符号表示为

$$p_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj} = \sum_{k} a_{ik} b_{kj}.$$

3
4

每一个这样的表达式都是(1.7)积矩阵定义中和的简化形式.

我们处理数集最重要的两个记号是上面所用的$\sum$(或求和记号)和矩阵记号. 实际上，记号$\sum$更为常用. 但由于矩阵记号更为紧凑，我们将尽可能地使用矩阵记号. 在后面几章中，我们的任务之一就是把复杂的数学结构转换成矩阵记号，从而方便地处理它们.

3

矩阵运算满足一些等式，如分配律

【1.10】 $$A(B+B')=AB+AB' \quad \text{和} \quad (A+A')B=AB+A'B$$

以及结合律

【1.11】 $$(AB)C=A(BC).$$

只要矩阵有适当的行列数使得运算能够进行，这些运算律就成立. 例如，对于结合律，要有正整数ℓ，m，n，p，使行列数为$A=\ell\times m$，$B=m\times n$，$C=n\times p$. 因为(1.11)中的两个积相等，所以括号可以省去而记为ABC. 这样三个矩阵的积ABC是一个$\ell\times p$矩阵. 例如，计算矩阵乘积

$$ABC=\begin{bmatrix}1\\2\end{bmatrix}\begin{bmatrix}1 & 0 & 1\end{bmatrix}\begin{bmatrix}2 & 0\\1 & 1\\0 & 1\end{bmatrix}$$

的两种方式为

$$(AB)C=\begin{bmatrix}1 & 0 & 1\\2 & 0 & 2\end{bmatrix}\begin{bmatrix}2 & 0\\1 & 1\\0 & 1\end{bmatrix}=\begin{bmatrix}2 & 1\\4 & 2\end{bmatrix}$$

和

$$A(BC)=\begin{bmatrix}1\\2\end{bmatrix}\begin{bmatrix}2 & 1\end{bmatrix}=\begin{bmatrix}2 & 1\\4 & 2\end{bmatrix}.$$

标量乘法与矩阵乘法相容，即有

【1.12】 $$c(AB)=(cA)B=A(cB).$$

这些等式的证明是很简单的，没有多大意义.

和结合律不同，矩阵乘法的交换律不成立；也就是说，

【1.13】 $$\text{通常 } AB\neq BA.$$

事实上，若A是$\ell\times m$矩阵，而B是$m\times\ell$矩阵，则AB和BA都有定义，但AB是$\ell\times\ell$矩阵而BA是$m\times m$矩阵. 即使是两个方阵，比如说$m\times m$矩阵，两个乘积也会不同. 例如，

5

$$\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}=\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}, \quad \text{而} \quad \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}.$$

矩阵乘法不可交换，在讨论矩阵方程时要多加注意. 当乘积有定义时，可以在方程$B=C$的两边左乘矩阵A而得到$AB=AC$. 同样，在乘积有定义时也可得到$BA=CA$. 但我们不能由$B=C$而得到$AB=CA$！

对任意大小的矩阵，如果其元素都是0，则称之为零矩阵，记为0. 也许记为$0_{m\times n}$更好.

矩阵A的元素a_{ii}称为对角元素，一个非零元素都是对角元素的矩阵称为对角矩阵.

非零元素是对角元素且每一个非零元素都为 1 的 $n\times n$ 方阵

【1.14】
$$I_n=\begin{bmatrix}1&0&\cdots&0\\0&1&\cdots&0\\\vdots&&\ddots&\vdots\\0&0&\cdots&1\end{bmatrix}$$

称为 $n\times n$ 单位矩阵. 它在乘法中的作用就像 1 一样：若 A 是一个 $m\times n$ 矩阵，则有

$$I_mA=A\quad 而\quad AI_n=A.$$

下面是两种表示单位矩阵 I_n 的简单方法：

$$I_n=\begin{bmatrix}1&&0\\&\ddots&\\0&&1\end{bmatrix}=\begin{bmatrix}1&&\\&\ddots&\\&&1\end{bmatrix}.$$

我们常用一块空白或单独一个 0 来表示矩阵中一整块为零的区域.

我们用 * 表示矩阵中任意的未定元素. 这样

$$\begin{bmatrix}*&&*\\&\ddots&\\0&&*\end{bmatrix}$$

表示一个对角线下面元素为 0，而其他元素未定的矩阵. 这样的矩阵称为上三角矩阵.

设 A 是一个 $n\times n$ 方阵. 若有矩阵 B 使得

【1.15】
$$AB=I_n\quad 且\quad BA=I_n,$$

则 B 称为 A 的逆，记作 A^{-1}：

【1.16】
$$A^{-1}A=I_n=AA^{-1}.$$

当 A 有逆时，称 A 为*可逆矩阵*. 例如，矩阵 $\begin{bmatrix}2&1\\5&3\end{bmatrix}$ 可逆. 其逆为 $A^{-1}=\begin{bmatrix}3&-1\\-5&2\end{bmatrix}$，直接计算 AA^{-1} 和 $A^{-1}A$ 就可以验证这一点. 另外两个例子是

6

$$\begin{bmatrix}1&\\&2\end{bmatrix}^{-1}=\begin{bmatrix}1&\\&\frac{1}{2}\end{bmatrix}\quad 和\quad \begin{bmatrix}1&1\\&1\end{bmatrix}^{-1}=\begin{bmatrix}1&-1\\&1\end{bmatrix}.$$

我们后面将看到，如果存在矩阵 B 使 $AB=I_n$ 和 $BA=I_n$ 这两个关系之一成立，则A 可逆，并且 B 就是 A 的逆[见(2.23)]. 由于矩阵乘法是不可交换的，所以这并不是显而易见的. 当矩阵不是方阵时就不成立. 例如，设 $A=[1\quad 2]$，$B=\begin{bmatrix}1\\0\end{bmatrix}$，则有 $AB=[1]=I_1$，但 $BA=\begin{bmatrix}1&2\\0&0\end{bmatrix}\neq I_2$.

另一方面，逆只要存在就是唯一的. 换言之，只能有唯一的逆. 设 B，B' 为两个对同一个矩阵 A 满足(1.15)的矩阵. 我们仅需知道 $AB=I_n$(B 是*右逆*)和 $B'A=I_n$(B' 是*左逆*). 由结合律，$B'(AB)=(B'A)B$. 于是

【1.17】
$$B'=B'I=B'(AB)=(B'A)B=IB=B,$$

因此 $B'=B$.

【1.18】命题 设 A，B 为 $n\times n$ 矩阵. 若两个矩阵都可逆，则其乘积 AB 也可逆，且有

$$(AB)^{-1}=B^{-1}A^{-1}.$$

更一般地，若 A_1，…，A_m 都可逆，则乘积 $A_1\cdots A_m$ 也可逆，并且其逆是 $A_m^{-1}\cdots A_1^{-1}$.

这样，$\begin{bmatrix}1&\\&2\end{bmatrix}\begin{bmatrix}1&1\\&1\end{bmatrix}=\begin{bmatrix}1&1\\&2\end{bmatrix}$的逆是$\begin{bmatrix}1&-1\\&1\end{bmatrix}\begin{bmatrix}1&\\&\frac{1}{2}\end{bmatrix}=\begin{bmatrix}1&-\frac{1}{2}\\&\frac{1}{2}\end{bmatrix}$.

证明 设 A，B 可逆，我们验证 $B^{-1}A^{-1}$是 AB 的逆：

$$ABB^{-1}A^{-1}=AIA^{-1}=AA^{-1}=I,$$

类似地

$$B^{-1}A^{-1}AB=\cdots=I.$$

最后一个断言可对 m 归纳证明[见附录(2.3)]. 当 $m=1$ 时，断言说，如果 A_1 可逆，则其逆为 A_1^{-1}，这是显然的. 然后假设断言对 $m=k$ 成立，并着手验证 $m=k+1$ 的情形. 假设A_1，…，A_{k+1}都是可逆 $n\times n$ 矩阵，用 P 记前 k 个矩阵的积 $A_1\cdots A_k$. 由归纳假设，P 可逆且其逆为 $A_k^{-1}\cdots A_1^{-1}$. 此外，A_{k+1} 可逆. 于是由我们所证明的两个可逆矩阵的情形，可以得到积 $PA_{k+1}=A_1\cdots A_kA_{k+1}$可逆，且其逆是 $A_{k+1}^{-1}P^{-1}=A_{k+1}^{-1}A_k^{-1}\cdots A_1^{-1}$. 这对 $m=k+1$ 证明了断言，从而完成了归纳证明. ■

7

我们将看到大多数矩阵是可逆的，虽然由矩阵乘法的定义这个事实并不明显. 但当矩阵很大时，具体找出其逆并不简单.

全部可逆的 $n\times n$ 矩阵的集合称为 n 维一般线性群，记作 GL_n. 在下一章我们学习群的基本概念时，一般线性群是最重要的例子之一.

在我们感兴趣的情形，有各种简化矩阵乘法的技巧. 分块乘法是其中之一. 设 M，M'分别为 $m\times n$ 和 $n\times p$ 矩阵，r 是小于 n 的整数. 可将两个矩阵如下分块：

$$M=[A\mid B]\quad 和\quad M'=\left[\frac{A'}{B'}\right],$$

其中 A 有 r 列，而 A'有 r 行. 矩阵乘积可如下计算：

【1.19】
$$MM'=AA'+BB'.$$

乘积的这种分解直接由定义得到并可以简化计算. 例如，

$$\left[\begin{array}{cc|c}1&0&5\\0&1&7\end{array}\right]\left[\begin{array}{cc}2&3\\4&8\\\hline 0&0\end{array}\right]=\begin{bmatrix}1&0\\0&1\end{bmatrix}\begin{bmatrix}2&3\\4&8\end{bmatrix}+\begin{bmatrix}5\\7\end{bmatrix}\begin{bmatrix}0&0\end{bmatrix}=\begin{bmatrix}2&3\\4&8\end{bmatrix}.$$

注意，公式(1.19)看起来与行向量和列向量相乘的规则(1.6)是一样的.

我们也可将矩阵分成更多块来乘. 一般来说，把矩阵分解成四块是最有用的. 这时，分块乘法的规则与 2×2 矩阵的乘法是一样的. 设 $r+s=n$，$k+\ell=m$. 假设将一个 $m\times n$ 矩阵 M 和一个 $n\times p$ 矩阵 M'分解成子矩阵

$$M=\left[\begin{array}{c|c}A & B\\ \hline C & D\end{array}\right],\quad M'=\left[\begin{array}{c|c}A' & B'\\ \hline C' & D'\end{array}\right],$$

其中 A 的列数等于 A' 的行数. 于是分块乘法规则为

【1.20】
$$\left[\begin{array}{c|c}A & B\\ \hline C & D\end{array}\right]\left[\begin{array}{c|c}A' & B'\\ \hline C' & D'\end{array}\right]=\left[\begin{array}{c|c}AA'+BC' & AB'+BD'\\ \hline CA'+DC' & CB'+DD'\end{array}\right].$$

例如,

$$\left[\begin{array}{cc|c}1 & 0 & 5\\ \hline 0 & 1 & 7\end{array}\right]\cdot\left[\begin{array}{cc|cc}2 & 3 & 1 & 1\\ 4 & 1 & 0 & 0\\ \hline 0 & 1 & 1 & 0\end{array}\right]=\left[\begin{array}{cc|cc}2 & 8 & 6 & 1\\ 4 & 8 & 7 & 0\end{array}\right].$$

8

在这个乘积中, 左上角块是 $[1\quad 0]\begin{bmatrix}2 & 3\\ 4 & 1\end{bmatrix}+[5][0\quad 1]=[2\quad 8]$等.

这一规则也可由矩阵乘法的定义直接验证. 一般来说, 只要矩阵能够分解成其所需乘积都有定义的子矩阵, 就可以用分块乘法.

除了可以简化计算外, 分块乘法也是用数学归纳法证明矩阵的有用工具.

第二节 行约简

设 $A=(a_{ij})$ 为 $m\times n$ 矩阵, 考虑 $n\times p$ 变量矩阵 $X=(x_{ij})$, 则矩阵方程

【2.1】
$$Y=AX$$

定义 $m\times p$ 矩阵 $Y=(y_{ij})$ 作为 X 的函数. 这个运算称为用 A 左乘:

【2.2】
$$y_{ij}=a_{i1}x_{1j}+a_{i2}x_{2j}+\cdots+a_{in}x_{nj}.$$

注意, 在公式(2.2)中元素 y_{ij} 仅依赖于 x_{1j}, …, x_{nj}, 即依赖于 X 的第 j 列和 A 的第 i 行. 因此 A 分别对 X 的每一列作用, 我们可以通过 A 对列向量的作用理解 A 的作用:

$$\boxed{A}\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}=\begin{bmatrix}y_1\\ \vdots\\ y_m\end{bmatrix}.$$

用 A 左乘列向量可以理解为一个从 n 维列向量空间 X 到 m 维列向量空间 Y 的函数, 或 m 个有 n 个变量的函数组:

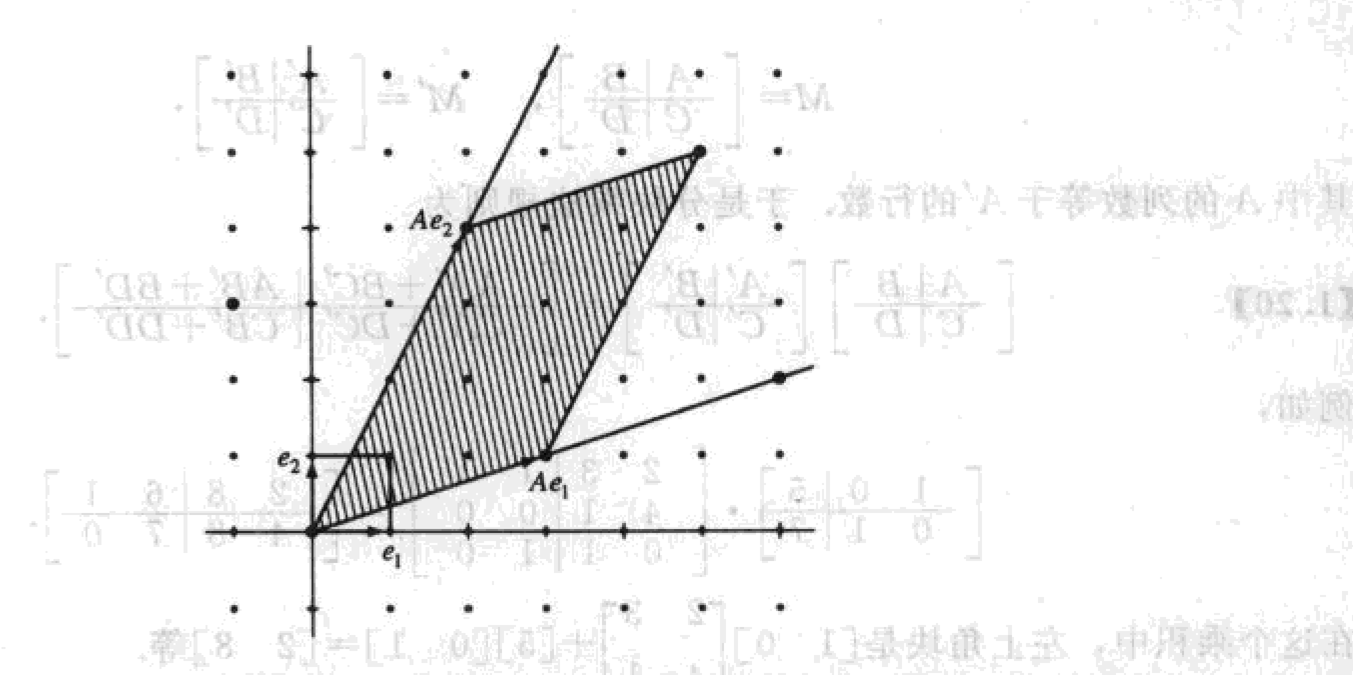
$$y_i=a_{i1}x_1+\cdots+a_{in}x_n\quad(i=1,\cdots,m).$$

由于这些函数是齐次的和线性的, 故称为线性变换. (变量集 u_1, …, u_k 上的线性函数是形如 $a_1u_1+\cdots+a_ku_k+c$ 的函数, 其中 a_1, …, a_k, c 是标量. 如果常数项 c 为零, 则这样的函数是齐次线性的.)

下面是 2×2 矩阵 $\begin{bmatrix}3 & 2\\ 1 & 4\end{bmatrix}$作用的图像, 它将二维空间映到二维空间:

9

【2.3】图



回到 A 在 $n\times p$ 矩阵 X 上的作用，A 对 X 的每一列的作用同样可以作如下解释：用 Y_i 表示 Y 的第 i 行，视之为行向量：

$$Y=\begin{bmatrix} - & Y_1 & - \\ - & Y_2 & - \\ & \vdots & \\ - & Y_p & - \end{bmatrix}$$

我们可用 X 的行 X_j 计算 Y_i，用向量记号表示，也就是

【2.4】
$$Y_i=a_{i1}X_1+\cdots+a_{in}X_n.$$

这其实是(2.2)的另一种写法，也是分块乘法的另一个例子. 例如，乘积

$$\begin{bmatrix} 0 & -1 & 2 \\ 3 & 4 & -6 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 4 & 2 \\ 3 & 2 \end{bmatrix}=\begin{bmatrix} 2 & 2 \\ 1 & -4 \end{bmatrix}$$

的底行可写为 $3[1\quad 0]+4[4\quad 2]-6[3\quad 2]=[1\quad -4]$.

当 A 为方阵时，我们常称用 A 左乘为行变换.

最简单的非零矩阵为矩阵单位，用 e_{ij} 表示：

【2.5】
$$e_{ij}=\begin{array}{cc} & \begin{matrix} & j & \end{matrix} \\ i & \begin{bmatrix} & \vdots & \\ \cdots & 1 & \cdots \\ & \vdots & \end{bmatrix} \end{array}.$$

10

矩阵 e_{ij} 在 (i,j) 位置的元素为 1，而其他所有位置的元素皆为 0.（我们通常用大写字母表示矩阵，但传统上用小写字母表示矩阵单位.）矩阵单位很有用，因为每个矩阵 $A=(a_{ij})$ 都可以按下列方式写为和的形式：

$$A=a_{11}e_{11}+a_{12}e_{12}+\cdots+a_{nn}e_{nn}=\sum_{i,j}a_{ij}e_{ij}.$$

求和符号下面的 i,j 表示对 i 的所有值和 j 的所有值求和. 例如，

$$\begin{bmatrix}3 & 2\\1 & 4\end{bmatrix}=\begin{bmatrix}3 & \\ & \end{bmatrix}+\begin{bmatrix} & 2\\ & \end{bmatrix}+\begin{bmatrix} & \\1 & \end{bmatrix}+\begin{bmatrix} & \\ & 4\end{bmatrix}=3e_{11}+2e_{12}+1e_{21}+4e_{22}.$$

这样的和称为矩阵 e_{ij} 的线性组合.

利用矩阵单位讨论矩阵的加法与标量乘法很方便. 但对于讨论矩阵的乘法，称为*初等矩阵*的方阵更有用. 初等矩阵共有三类：

【2.6i】

$$\begin{bmatrix}1 & & a\\ & \ddots & \\ & & 1\end{bmatrix}\ 或\ \begin{bmatrix}1 & & \\ & \ddots & \\ a & & 1\end{bmatrix}=I+ae_{ij}\quad(i\neq j).$$

这样的矩阵对角线上的元素皆为 1 并有一个非 0 非对角元素.

【2.6ii】

$$\begin{bmatrix}1 & & & & & \\ & \ddots & & & & \\ & & 0 & & 1 & \\ & & & \ddots & & \\ & & 1 & & 0 & \\ & & & & & \ddots \\ & & & & & & 1\end{bmatrix}=I+e_{ij}+e_{ji}-e_{ii}-e_{jj}.$$

这里，I 的第 i 个和第 j 个对角元素用 0 代替，而在 $(i,\ j)$ 和 $(j,\ i)$ 位置各加上一个 1.（用矩阵单位的公式很难看，我们不会用得太多.）

【2.6iii】

$$\begin{bmatrix}1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & c & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1\end{bmatrix}=I+(c-1)e_{ii}\quad(c\neq 0).$$

由单位矩阵的一个对角元素被非零数 c 代替得到.

11

2×2 初等矩阵有

$$\text{(i)}\begin{bmatrix}1 & a\\0 & 1\end{bmatrix},\begin{bmatrix}1 & 0\\a & 1\end{bmatrix},\quad \text{(ii)}\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix},\quad \text{(iii)}\begin{bmatrix}c & \\ & 1\end{bmatrix},\begin{bmatrix}1 & \\ & c\end{bmatrix},$$

和上面一样，这里 a 任意，而 c 是任意非零数.

下面描述初等矩阵 E 在矩阵 X 上的作用.

【2.7】 要得到矩阵 EX，必须：

(i)型：用 $X_i+a\,X_j$ 代替第 i 行 X_i，或将 $a\cdot$(行 j)加到(行 i).

(ii)型：交换(行 i)与(行 j).

(iii)型：(行 i)乘上非零标量 c.

这些变换称为初等行变换．这样，左乘一个初等矩阵是一个初等行变换．读者应该仔细地验证乘法的这些规则．

【2.8】引理 *初等矩阵可逆，且其逆也是初等矩阵．*

证明 用计算就可证明这个引理．初等矩阵的逆是对应于逆行变换的矩阵：若 $E=I+ae_{ij}$ 为(i)型，则 $E^{-1}=I-ae_{ij}$，即"从(行 i)减去 $a\cdot$(行 j)"．若 E 为(ii)型，则 $E^{-1}=E$．若 E 为(iii)型，则 E^{-1} 为同型，用 c^{-1} 替代 c 在 E 中的位置得到，即"用 c^{-1} 乘(行 i)"． ■

下面讨论在矩阵 A 上行变换(2.7)的效果，目标是最终得到更为简单的矩阵 A'：

$$A \xrightarrow{\text{变换序列}} \rightarrow \cdots \rightarrow A'.$$

因为每个初等行变换可用一个初等矩阵左乘得到，所以可将一系列这样变换的结果表达为用一序列初等矩阵左乘：

【2.9】
$$A' = E_k \cdots E_2 E_1 A.$$

这一过程称为行约简或高斯消元法．例如，矩阵

【2.10】
$$M = \begin{bmatrix} 1 & 0 & 2 & 1 & 5 \\ 1 & 1 & 5 & 2 & 7 \\ 1 & 2 & 8 & 4 & 12 \end{bmatrix}$$

12 可用(i)型初等变换消去尽可能多的非零元素而得到化简：

$$\begin{bmatrix} 1 & 0 & 2 & 1 & 5 \\ 1 & 1 & 5 & 2 & 7 \\ 1 & 2 & 8 & 4 & 12 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 2 & 1 & 5 \\ 0 & 1 & 3 & 1 & 2 \\ 1 & 2 & 8 & 4 & 12 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 2 & 1 & 5 \\ 0 & 1 & 3 & 1 & 2 \\ 0 & 2 & 6 & 3 & 7 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 0 & 2 & 1 & 5 \\ 0 & 1 & 3 & 1 & 2 \\ 0 & 0 & 0 & 1 & 3 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 2 & 0 & 2 \\ 0 & 1 & 3 & 0 & -1 \\ 0 & 0 & 0 & 1 & 3 \end{bmatrix}.$$

行约简是解线性方程组的有用方法．设有由 m 个有 n 个未知量的方程组成的线性方程组，比如说 $AX=B$，如(1.9)，其中 A 是 $m\times n$ 矩阵，X 为未知列向量，而 B 为给定的列向量．为解这个方程组，我们构造 $m\times(n+1)$ 块矩阵

【2.11】
$$M = [A \mid B] = \left[\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_n \end{array}\right],$$

用行变换化简 M．注意到 $EM=[EA \mid EB]$．令

$$M' = [A' \mid B']$$

为一系列行变换的结果．关键的事实是：

【2.12】命题 $A'X=B'$ 与 $AX=B$ 同解．

证明 由于 M' 可由一系列初等行变换得到，故

$$M' = E_r \cdots E_1 M.$$

令 $P=E_r\cdots E_1$，由引理(2.8)及命题(1.18)，这是一个可逆矩阵．又 $M'=[A' \mid B']=[PA \mid PB]$．若 X 是原方程组 $AX=B$ 的解，则 $PAX=PB$，即 $A'X=B'$．从而 X 也是新方程组的解．反

之，若 $A'X=B'$，则 $AX=P^{-1}A'X=P^{-1}B'=B$，于是 X 也是方程组 $AX=B$ 的解. ■

例如，考虑方程组

【2.13】

$$\begin{aligned} x_1 \quad\quad + 2x_3 + x_4 &= 5 \\ x_1 + x_2 + 5x_3 + 2x_4 &= 7 \\ x_1 + 2x_2 + 8x_3 + 4x_4 &= 12. \end{aligned}$$

其增广矩阵是上面的(2.10)考虑的矩阵 M，从而行约简表明这一方程组等价于

$$\begin{aligned} x_1 \quad + 2x_3 \quad\quad &= 2 \\ x_2 + 3x_3 + \quad &= -1 \\ x_4 &= 3. \end{aligned}$$

13

我们可立即得到该方程组的解：可任取 x_3，然后解出 x_1，x_2 和 x_4. (2.13)的一般解可以写为

$$x_3=c_3, x_1=1-2c_3, x_2=-1-3c_3, x_4=3$$

的形式，其中 c_3 是任意的.

回到一个任意矩阵的行约简. 不难看出，任意矩阵 A 可经过一系列行约简而化为大致如下的形式：

【2.14】

$$A=\begin{bmatrix} 1 & *\cdots* & 0 & *\cdots* & 0 & *\cdots* & 0 & \\ & & 1 & *\cdots* & 0 & *\cdots* & 0 & \\ & & & & 1 & *\cdots* & 0 & \cdots \\ & & & & & & 1 & \\ & & & & & & & \ddots \end{bmatrix},$$

其中 * 表示任意数，而大块的空白表示 0. 这称为行阶梯矩阵. 例如

$$\begin{bmatrix} 1 & 6 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

是一个行阶梯矩阵. (2.10)最终的约简结果也是行阶梯矩阵.

行阶梯矩阵的定义如下：

【2.15】

(a) 每行的第一个非零元为 1，称之为主元.

(b) 第 $i+1$ 行的第一个非零元在第 i 行的第一个非零元的右边.

(c) 主元上面的元皆为零.

作行约简时，先找到有非零元的第一列. (如果没有，则 $A=0$，而 0 是行阶梯矩阵.)用(ii)型初等行变换交换行，使其中一个非零元移到顶行. 用(iii)型变换将该元正规化为 1. 然后用一系列(i)型行变换将该列其他元清零. 得到块矩阵 $\left[\begin{array}{ccc|c|ccc} 0 & \cdots & 0 & 1 & * & \cdots & * \\ \hline 0 & \cdots & 0 & 0 & * & \cdots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & * & \cdots & * \end{array}\right]$，可

14

将它写为 $\left[\begin{array}{c|c|c} & 1 & B \\ \hline & & D \end{array}\right]=A'$.继续对小矩阵 D 进行行变换(直到做完为止). 形式上，这是对矩阵

的大小进行归纳. 利用归纳法[见附录(2.6)], 可以假设每一行数比 A 的行数少的矩阵可约简为行阶梯形. 由于 D 的行数少, 故可设它能被约简为阶梯形, 记为 D'. 用于将 D 约简为 D''的行变换不会改变 A'中的其他块. 于是 A'可以约简为一个满足行阶梯矩阵要求(2.15a 和 b)的矩阵:

$$\left[\begin{array}{c|c|c} & 1 & B \\ \hline & & D'' \end{array}\right] = A'',$$

因而原来的矩阵 A 也可约简为这样的形式. 这时, 可将 D''主元上方的 B 中的元清零, 而最终约简得到一个行阶梯矩阵. ■

可以证明, 由给定矩阵 A 经过行约简得到的行阶梯矩阵是唯一的, 即与所用的行变换序列无关. 然而这不太重要, 这里省去其证明.

使用行约简的原因是, 当 A'是一个行阶梯矩阵时, 可以立即解出线性方程组 $A'X=B'$. 例如, 设

$$[A' \mid B'] = \left[\begin{array}{cccc|c} 1 & 6 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right].$$

由于第三个方程是 $0=1$, 因而方程 $A'X=B'$无解. 另一方面,

$$[A' \mid B'] = \left[\begin{array}{cccc|c} 1 & 6 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

有解. 任取 x_2, x_4, 可由第一个方程解出 x_1, 由第二个方程解出 x_3. 这正是我们用来解方程组(2.13)的过程.

一般的法则如下:

【2.16】命题 设 $M'=[A' \mid B']$为行阶梯矩阵. 则线性方程组 $A'X=B'$有解的充分必要条件是最后一列 B'没有主元. 这时, 如果第 i 列没有主元, 则未知量 x_i 可取任意值.

15

齐次线性方程组 $AX=0$ 当然有平凡解 $X=0$. 从行阶梯形又可看出, 当未知量个数大于方程个数时, 齐次线性方程组 $AX=0$ 必有一个非平凡解 X:

【2.17】推论 当 $m<n$ 时, 每一个由 m 个有 n 个未知量的方程组成的齐次线性方程组有一个使某个 x_i 非零的解 X.

设 $A'X=0$ 为相应的行阶梯方程, 设 r 为 A'的主元的个数. 则 $r\leqslant m$. 根据命题, 我们可以对 $n-r$ 个变量 x_i 取任意值. ■

现在我们用行约简刻画可逆方阵.

【2.18】命题 设 A 为方阵, 则下列条件等价:

(a) A 可以由一系列初等行变换约简为单位矩阵.

(b) A 是初等矩阵的积.

(c) A 可逆.

(d) 齐次线性方程组 $AX=0$ 仅有平凡解 $X=0$.

证明 我们通过证明(a)⇒(b)⇒(c)⇒(d)⇒(a)来证明命题. 要证(a)推出(b), 设 A 可由

初等行变换约简为单位矩阵：$E_k \cdots E_1 A = I$. 在这个式子两边乘上 $E_1^{-1} \cdots E_k^{-1}$，得 $A = E_1^{-1} \cdots E_k^{-1}$. 因为初等矩阵的逆仍是初等矩阵，所以 A 是初等矩阵的乘积. 由于初等矩阵的乘积可逆，因此由(b)推出(c). 若 A 可逆，在方程 $AX=0$ 两边乘 A^{-1} 得 $X=0$. 故方程 $AX=0$ 仅有平凡解. 因而由(c)推出(d).

最后要证由(d)推出(a)，考察行阶梯方阵 A. 注意下面的情形：

【2.19】*设 M 为行阶梯方阵. 则 M 或为单位矩阵，或其底行为零.*

这容易由(2.15)看出.

设(a)对给定的矩阵 A 不成立. 则 A 可用行变换化成一个底行为零的矩阵 A'. 这时，线性方程组 $A'X=0$ 中只有 $n-1$ 个非平凡的线性方程，因而由推论(2.17)可知这个方程组有非零解. 因为方程组 $AX=0$ 等价于方程组 $A'X=0$，所以它也有非平凡解. 这表明若(a)不成立，则(d)也不成立，从而(d)推出(a). 这就证明了命题(2.18). ■

16

【2.20】推论 *若方阵 A 有一行为零，则 A 不可逆.*

行约简给出了一种计算可逆矩阵 A 的逆的办法：像前面一样，用行变换把 A 约简为单位矩阵：

$$E_k \cdots E_1 A = I$$

在其两边右乘 A^{-1}，我们有

$$E_k \cdots E_1 I = A^{-1}.$$

【2.21】推论 *设 A 是可逆矩阵. 要计算其逆 A^{-1}，先在 A 上用初等行变换 $E_1, \cdots, E_k$ 把它约简为单位矩阵. 当同一系列初等行变换用于 I 时，得到 A^{-1}.*

这个推论只不过是上面两个等式的复述.

【2.22】例 求矩阵

$$A = \begin{bmatrix} 5 & 4 \\ 6 & 5 \end{bmatrix}$$

的逆.

先构造 2×4 块矩阵

$$[A/I] = \left[\begin{array}{cc|cc} 5 & 4 & 1 & 0 \\ 6 & 5 & 0 & 1 \end{array}\right].$$

对矩阵 A 作行变换将其化为单位矩阵，右边也同时作行变换，则由推论(2.21)，最终右边化为 A^{-1}.

$$[A \mid I] = \left[\begin{array}{cc|cc} 5 & 4 & 1 & 0 \\ 6 & 5 & 0 & 1 \end{array}\right] \quad \text{从(行 2) 减去(行 1)}$$

$$\to \left[\begin{array}{cc|cc} 5 & 4 & 1 & 0 \\ 1 & 1 & -1 & 1 \end{array}\right] \quad \text{从(行 1) 减去 4·(行 2)}$$

$$\to \left[\begin{array}{cc|cc} 1 & 0 & 5 & -4 \\ 1 & 1 & -1 & 1 \end{array}\right] \quad \text{从(行 2) 减去(行 1)}$$

$$\to \left[\begin{array}{cc|cc} 1 & 0 & 5 & -4 \\ 0 & 1 & -6 & 5 \end{array}\right] = [I \mid A^{-1}]$$

于是 $A^{-1} = \begin{bmatrix} 5 & -4 \\ -6 & 5 \end{bmatrix}$.

【2.23】命题 设 A 为方阵，有左逆 B：$BA=I$ 或右逆 B：$AB=I$. 则 A 可逆，且 B 为其逆.

证明 设 $AB=I$. 我们对 A 作行约简. 根据(2.19)，有初等矩阵 E_1，…，E_k，使 $A'=E_k\cdots E_1A$ 为单位矩阵或底行为零. 则 $A'B=E_k\cdots E_1$ 是可逆矩阵. 于是 $A'B$ 的底行非零，从而 A' 的底行亦非零. 由此得 $A'=I$. 由(2.18)，A 可逆，由方程 $I=E_k\cdots E_1A$ 及 $AB=I$ 得 $A^{-1}=E_k\cdots E_1=B$ (见(1.17)). 另一情形为 $BA=I$，可在上面的推理中交换 A 与 B 的位置得到 B 可逆且 A 是它的逆. 因此 A 也可逆. ■

17

我们讨论的大部分内容，可以用列代替行进行. 之所以选择讨论行，是为了将结果应用于线性方程组，否则选择列也是一样的. 通过矩阵*转置*使行列互换. $m\times n$ 矩阵 A 的转置 A^t 是通过将它关于对角线作反射得到的 $n\times m$ 矩阵：$A^t=(b_{ij})$，其中

$$b_{ij}=a_{ji}.$$

例如，

$$\begin{bmatrix}3 & 2\\ 1 & 4\end{bmatrix}^t=\begin{bmatrix}3 & 1\\ 2 & 4\end{bmatrix} \quad 及 \quad [1\ \ 2\ \ 3]^t=\begin{bmatrix}1\\ 2\\ 3\end{bmatrix}.$$

计算转置的法则由(2.24)给出.

【2.24】

(a) $(A+B)^t=A^t+B^t$.

(b) $(cA)^t=cA^t$.

(c) $(AB)^t=B^tA^t$!

(d) $(A^t)^t=A$.

利用公式(2.24c 和 d)，可由关于左乘的相应事实得到关于*右乘* XP 的事实.

用初等矩阵(2.6)右乘的作用是下列*初等列变换*：

【2.25】

(a) 将 $a\cdot$(列 i)加到(列 j).

(b) 交换(列 i)与(列 j).

(c) 用 $c\neq0$ 乘(列 i).

第三节 行 列 式

每一个方阵 A 都有一个数与之对应，这个数称为*行列式*. 本节定义行列式并推出它的一些性质. 矩阵 A 的行列式将记为 $\det A$.

18

1×1 矩阵的行列式就是其唯一元素

【3.1】
$$\det[a]=a,$$

2×2 矩阵的行列式为

【3.2】
$$\det\begin{bmatrix}a & b\\ c & d\end{bmatrix}=ad-bc.$$

如果像第二节中一样把 2×2 矩阵 A 视为二维实向量空间 $\mathbb{R}^2$ 的线性算子，则可从几何上解释

行列式 $\det A$. 它的绝对值是单位方形在作用下的像形成的平行四边形的面积. 例如，图(2.3)的阴影部分的面积是 10. 根据正方形的方向在作用后是保持还是相反，行列式为正或负. 此外，$\det A=0$ 当且仅当平行四边形退化为一条线段，当且仅当 A 的两列成比例这才会发生.

全体 $n\times n$ 矩阵构成一个 n^2 维向量空间，记作$\mathbb{R}^{n\times n}$. 我们将视 $n\times n$ 矩阵的行列式为此空间到实数的一个*函数*：

$$\det:\mathbb{R}^{n\times n}\longrightarrow\mathbb{R}.$$

这意味着行列式是 n^2 个矩阵元素的函数. 对每一正整数 n 有一个这样的函数. 有许多计算行列式的公式，可是，当 n 较大时它们全部都很复杂. 虽然没有简单的公式来计算行列式，但由于它有很好的性质，故很重要. 行列式不仅计算公式复杂，而且也不容易直接证明两个行列式定义的是同一个函数. 因而，我们将采用下面的策略：本质上随机地选择一个公式作为行列式的定义. 这样，所讨论的是一个特定的函数. 我们证明所选择的函数有某些非常特殊的性质. 我们还证明所选择的函数是*仅有的*满足这些性质的函数. 于是，要验证明某个其他公式定义的是同一个行列式，只需证明它定义的函数具有这些同样的性质. 事实表明，这通常相对容易一些.

20

一个 $n\times n$ 矩阵的行列式可根据某些$(n-1)\times(n-1)$行列式用*关于子式展开*的过程计算. 利用这种展开，给出行列式函数的一个递归定义. 设 A 为 $n\times n$ 矩阵，而用 A_{ij} 表示在 A 中删去第 i 行和第 j 列得到的$(n-1)\times(n-1)$矩阵：

【3.3】 （图：矩阵中第 i 行、第 j 列被划去） $= A_{ij}$.

19

例如，若

$$A=\begin{bmatrix}1&0&3\\2&1&2\\0&5&1\end{bmatrix},\quad 则\quad A_{21}=\begin{bmatrix}0&3\\5&1\end{bmatrix}.$$

在第一列对子式展开由下式给出：

【3.4】 $$\det A=a_{11}\det A_{11}-a_{21}\det A_{21}+,-\cdots\pm a_{n1}\det A_{n1}.$$

符号是交错的. 这一公式与(3.1)一起组成*行列式的递归定义*. 对 2×2 矩阵，这个公式与(3.2)是一致的.

上面给出的矩阵 A 的行列式为

$$\det A=1\cdot\det\begin{bmatrix}1&2\\5&1\end{bmatrix}-2\cdot\det\begin{bmatrix}0&3\\5&1\end{bmatrix}+0\cdot\det\begin{bmatrix}0&3\\1&2\end{bmatrix}.$$

这里出现的三个 2×2 矩阵可再对子式展开后用(3.1)或(3.2)计算，得到

$$\det A=1\cdot(-9)-2\cdot(-15)+0\cdot(-3)=21.$$

后面将推出行列式的一些其他公式，包括在其他列或行对子式展开[见(4.11)、(5.1)、(5.2)].

无论是从行列式的计算上还是从理论上，知道行列式所满足的一些性质都是重要的. 其中大多数可用关于子式展开(3.4)直接计算和对 n 作归纳来证明. 对一些性质，我们只列出它们但不给出正式证明. 为了能对除行列式之外的其他函数解释这些性质，我们将暂时用符号 d 来表示行列式.

【3.5】 $$\mathrm{d}(I)=1.$$

【3.6】函数 $\mathrm{d}(A)$ 对矩阵的各行是线性的.

其意义如下：设 R_i 为矩阵的第 i 行构成的行向量，则从符号上 A 可写作

$$A=\begin{bmatrix} —R_1— \\ \vdots \\ —R_n— \end{bmatrix}.$$

由定义，在第 i 行的线性性是指，如果 R 和 S 是行向量，则

$$\mathrm{d}\begin{bmatrix} \vdots \\ —R+S— \\ \vdots \end{bmatrix}=\mathrm{d}\begin{bmatrix} \vdots \\ —R— \\ \vdots \end{bmatrix}+\mathrm{d}\begin{bmatrix} \vdots \\ —S— \\ \vdots \end{bmatrix},$$

$$\mathrm{d}\begin{bmatrix} \vdots \\ —cR— \\ \vdots \end{bmatrix}=c\mathrm{d}\begin{bmatrix} \vdots \\ —R— \\ \vdots \end{bmatrix},$$

其中，这些关系中的矩阵的其余行始终不变. 例如，

$$\det\begin{bmatrix} 1 & 2 & 4 \\ 3+5 & 4+6 & 2+3 \\ 2 & -1 & 0 \end{bmatrix}=\det\begin{bmatrix} 1 & 2 & 4 \\ 3 & 4 & 2 \\ 2 & -1 & 0 \end{bmatrix}+\det\begin{bmatrix} 1 & 2 & 4 \\ 5 & 6 & 3 \\ 2 & -1 & 0 \end{bmatrix},$$

$$\det\begin{bmatrix} 1 & 2 & 4 \\ 2\cdot 5 & 2\cdot 6 & 2\cdot 3 \\ 2 & -1 & 0 \end{bmatrix}=2\cdot\det\begin{bmatrix} 1 & 2 & 4 \\ 5 & 6 & 3 \\ 2 & -1 & 0 \end{bmatrix}.$$

线性性使我们能每次对一行进行处理而保持其他行不变.

另一个性质：

【3.7】若矩阵 A 的两个相邻行相等，则 $\mathrm{d}(A)=0$.

我们对 n 作归纳证明这一事实. 设 j 行与 $j+1$ 行相等. 那么，除了 $i=j$ 和 $i=j+1$，在(3.3)定义的矩阵 A_{i1} 中必有两行相等. 由归纳假设，当 A_{i1} 有两行相等时，其行列式为零. 于是(3.4)中只有两项非零，即

$$\mathrm{d}(A)=\pm a_{j1}\mathrm{d}(A_{j1})\mp a_{(j+1)1}\mathrm{d}(A_{(j+1)1}).$$

此外，由于行 R_j 与 R_{j+1} 相等，于是 $A_{j1}=A_{(j+1)1}$ 且 $a_{j1}=a_{(j+1)1}$. 而右边两项符号相反，它们互相抵消，所以行列式为零.

性质(3.5)～(3.7)唯一地刻画了行列式[见(3.14)]，我们将不必回到(3.4)而直接由它们推导出更多的关系.

【3.8】若一行的倍数加到邻行，则行列式不变.

例如，由(3.6)和(3.7)，

$$\mathrm{d}\begin{bmatrix} \vdots \\ \text{——}R\text{——} \\ \text{——}S+cR\text{——} \\ \vdots \end{bmatrix} = \mathrm{d}\begin{bmatrix} \vdots \\ \text{——}R\text{——} \\ \text{——}S\text{——} \\ \vdots \end{bmatrix} + c\mathrm{d}\begin{bmatrix} \vdots \\ \text{——}R\text{——} \\ \text{——}R\text{——} \\ \vdots \end{bmatrix} = \mathrm{d}\begin{bmatrix} \vdots \\ \text{——}R\text{——} \\ \text{——}S\text{——} \\ \vdots \end{bmatrix}.$$

21

同理，S 行在 R 行的上面时也成立.

【3.9】 *若交换相邻两行，则行列式乘 -1.*

重复使用(3.8)，得

$$\mathrm{d}\begin{bmatrix} \vdots \\ \text{——}R\text{——} \\ \text{——}S\text{——} \\ \vdots \end{bmatrix} = \mathrm{d}\begin{bmatrix} \vdots \\ \text{——}R\text{——} \\ \text{——}(S-R)\text{——} \\ \vdots \end{bmatrix} = \mathrm{d}\begin{bmatrix} \vdots \\ \text{——}R+(S-R)\text{——} \\ \text{——}(S-R)\text{——} \\ \vdots \end{bmatrix}$$

$$= \mathrm{d}\begin{bmatrix} \vdots \\ \text{——}S\text{——} \\ \text{——}(S-R)\text{——} \\ \vdots \end{bmatrix} = \mathrm{d}\begin{bmatrix} \vdots \\ \text{——}S\text{——} \\ \text{——}(-R)\text{——} \\ \vdots \end{bmatrix} = -\mathrm{d}\begin{bmatrix} \vdots \\ \text{——}S\text{——} \\ \text{——}R\text{——} \\ \vdots \end{bmatrix}.$$

【3.7′】 *若矩阵 A 的两行相等，则 $\mathrm{d}(A)=0$.*

因为交换相邻两行若干次，得到有相邻两行相等的矩阵 A'. 由(3.7)，$\mathrm{d}(A')=0$，再由(3.9)，$\mathrm{d}(A)=\pm\mathrm{d}(A')$.

利用(3.7)，由(3.8)和(3.9)的证明得到下面的结果：

【3.8′】 *若一行的倍数加到另一行，则行列式不变.*

【3.9′】 *若交换两行，则行列式乘 -1.*

而由(3.6)可以得到下面的结果：

【3.10】 *若 A 的一行为零，则 $\mathrm{d}(A)=0$.*

若一行为零，则当该行乘以零时 A 不变. 由(3.6)，它等于 $\mathrm{d}(A)$ 乘以 0. 这样 $\mathrm{d}(A)=0\mathrm{d}(A)=0$.

规则(3.8′)、(3.9′)和(3.6)描述了初等行变换(2.7)对行列式作用后的效果，因而可通过初等矩阵重新写出. 这告诉我们，若 E 为第一类初等矩阵，则 $\mathrm{d}(EA)=\mathrm{d}(A)$；若 E 是第二类初等矩阵，则 $\mathrm{d}(EA)=-\mathrm{d}(A)$；若 E 是第三类初等矩阵，则 $\mathrm{d}(EA)=c\mathrm{d}(A)$. 我们用这些规则来计算初等矩阵 E 的 $\mathrm{d}(E)$. 替换 $A=I$，则由于 $\mathrm{d}(I)=1$，根据上面的规则可得 $\mathrm{d}(EI)=\mathrm{d}(E)$：

22

【3.11】 *初等矩阵的行列式为：*

(i) 第一类(一行的倍数加到另一行)：$\mathrm{d}(E)=1$，由(3.8′)得到.

(ii) 第二类(行交换)：$\mathrm{d}(E)=-1$，由(3.9′)得到.

(iii) 第三类(一行乘上一个非零数)：$\mathrm{d}(E)=c$，由(3.6′)得到.

现在，把规则(3.8′)、(3.9′)及(3.6)应用于一个任意矩阵 A，并利用我们刚才确定的 $\mathrm{d}(E)$ 的值，得到下面的结果：

【3.12】 *设 E 是初等矩阵且 A 是任意矩阵，则*

$$\mathrm{d}(EA)=\mathrm{d}(E)\mathrm{d}(A).$$

回忆由(2.19)，任一方阵 A 可用初等行变换约简为一个矩阵 A'，它或者是单位矩阵 I，或者底行为零：

$$A' = E_k \cdots E_1 A.$$

由(3.5)和(3.10)，我们知道在这两种情形分别有 $d(A')=1$ 和 $d(A')=0$. 由(3.12)及数学归纳法，

【3.13】
$$d(A') = d(E_k)\cdots d(E_1)d(A).$$

由(3.11)，我们知道 $d(E_i)$ 的取值，因而可用这个公式计算 $d(A)$.

【3.14】定理 *行列式的公理刻画：行列式函数(3.4)是满足性质(3.5)～(3.7)的仅有的函数.*

证明 只用这些规则就能得到(3.11)和(3.13)，而这两个等式唯一确定 $d(A)$. 关于子式展开(3.4)满足(3.5)～(3.7)，从而也满足(3.13). ■

我们仍用 $\det A$ 表示一个矩阵的行列式.

【3.15】推论 *方阵 A 可逆当且仅当 $\det A\neq 0$.*

这可由公式(3.11)、(3.13)和(2.18)得到. 由(3.11)，对所有 i 有 $\det E_i\neq 0$. 因此，如果 A' 如(3.13)中给出，则 $\det A\neq 0$ 当且仅当 $\det A'\neq 0$，而这成立当且仅当 $A'=I$. 由(2.18)，$A'=I$ 当且仅当 A 可逆.

我们现在证明行列式函数最重要的性质之一，即它与矩阵乘法的相容性.

【3.16】定理 *设 A，B 为任意两个 $n\times n$ 矩阵. 则*

23

$$\det(AB) = (\det A)(\det B).$$

证明 注意当 A 为初等矩阵时，这就是(3.12).

情形 1：A 可逆. 由(2.18b)，A 是初等矩阵的乘积：$A=E_1\cdots E_k$. 由(3.12)及数学归纳法，$\det A=(\det E_1)\cdots(\det E_k)$，故

$$\det(AB) = \det(E_1\cdots E_k B) = (\det E_1)\cdots(\det E_k)(\det B) = (\det A)(\det B).$$

情形 2：A 不可逆. 则由(3.15)，$\det A=0$，如果我们能证明这时 $\det(AB)=0$，则定理成立. 由(2.18)，A 可以约简为一个底行为零的矩阵 $A'=E_k\cdots E_1 A$. 从而 $A'B$ 的底行也为零. 于是

$$0 = \det(A'B) = \det(E_k\cdots E_1 AB) = (\det E_k)\cdots(\det E_1)(\det AB).$$

因为 $\det E_i\neq 0$，从而 $\det(AB)=0$. ■

【3.17】推论 *若 A 可逆，则 $\det A^{-1}=\dfrac{1}{\det A}$.*

证明 $(\det A)(\det A^{-1})=\det I=1$. ■

注意 使用规则(3.11)和(3.16)来定义行列式是很自然的想法. 因为每一可逆矩阵 A 可以写成初等矩阵的乘积，对每个可逆矩阵，这些规则当然定义了其行列式. 但其中有问题，即每个矩阵可以有许多方式写成初等矩阵的乘积. 如果不通过上面证明中的步骤，我们并不清楚两个不同的乘积是否给出相同的行列式. 实际上要使这种想法得以实现并不特别容易.

下列命题的证明是个很好的练习.

【3.18】命题 *用 A^t 表示 A 的转置，则*

$$\det A = \det A^{t}.$$

【3.19】推论 如果(3.6)～(3.10)中的所有“行”字换成“列”字，性质(3.6)～(3.10)仍成立.

第四节 置换矩阵

24

集合 S 到自身的一个双射 p 称为该集合的一个置换：

【4.1】
$$p: S \longrightarrow S.$$

例如，

【4.2】
$$\begin{aligned} 1 &\rightsquigarrow 3 \\ 2 &\rightsquigarrow 1 \\ 3 &\rightsquigarrow 2 \end{aligned}$$

是集合{1，2，3}的一个置换. 因为其作用为

$$1 \to 2 \to 3 \to 1,$$

所以称之为循环置换.

置换可用多种记号表示. 本节采用函数记号，这样 $p(x)$ 表示置换 p 在元素 x 上的取值. 因此，若 p 是(4.2)给出的置换，则

$$p(1) = 3, \quad p(2) = 1, \quad p(3) = 2.$$

置换矩阵 P 是具有下列性质的矩阵：P 左乘的作用是矩阵的行的一个置换. 第二类初等矩阵(2.6ii)是最简单的例子. 它们对应于称为对换的置换，即交换矩阵的两行而其余行不动.

【4.3】
$$P = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

也是置换矩阵，它对列向量 $X = (x, y, z)^{t}$ 的作用为

$$PX = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} y \\ z \\ x \end{bmatrix}.$$

第一个位置的元素变到了第三个位置，等等，因而 P 按(4.2)的循环置换 p 给出的方式置换各行.

有一种情形会引起混乱，这种情形要求我们仔细使用记号. 当用置换 p 置换向量 $(x_1, \cdots, x_n)^{t}$ 的元素时，指标以相反方式置换. 例如，用(4.3)的矩阵乘列向量 $X = (x_1, x_2, x_3)^{t}$，得

【4.4】
$$PX = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \end{bmatrix}.$$

(4.4)中的指标由 $1 \rightsquigarrow 2 \rightsquigarrow 3 \rightsquigarrow 1$ 置换，这是置换 p 的逆. 这样，将置换联系到置换矩阵 P 的方式有两种：置换 p 刻画 P 如何置换元素，而 p 的逆刻画 P 在指标上作用的效果. 我们必须做出选择，因此把与 P 相对应的置换说成是刻画它在列向量元素上作用的那个置换. 于是，对指标的作用是以相反方式进行的，从而

【4.5】
$$PX=\begin{bmatrix}x_{p^{-1}(1)}\\ \vdots\\ x_{p^{-1}(n)}\end{bmatrix}.$$

25

用 P 乘相当于在 $n\times r$ 矩阵 A 的行上作用的效果.

置换矩阵 P 可以方便地用矩阵单位(2.5)写出，或用称为标准基并记作 e_i 的列向量写出. 向量 e_i 在第 i 个位置有单一非零元 1，因而这些向量是 $n\times 1$ 矩阵的矩阵单位.

【4.6】命题 设 P 是与置换 p 相应的置换矩阵.

(a) P 的第 j 列为列向量 $e_{p(j)}$.

(b) P 是 n 个矩阵单位的和：$P=e_{p(1)1}+\cdots+e_{p(n)n}=\sum_j e_{p(j)j}$.

置换矩阵 P 在每一行和每一列中总有单独一个 1，其余元皆为 0. 反之，任一这样的矩阵都是一个置换矩阵.

【4.7】命题

(a) 设 p，q 为两个置换，相应的置换矩阵为 P，Q. 则置换 pq 相应的置换矩阵为积 PQ.

(b) 置换矩阵 P 可逆，并且其逆为转置矩阵：$P^{-1}=P^t$.

证明 pq 是指两个置换的合成

【4.8】
$$pq(i)=p(q(i)).$$

因为 P 的作用是按 p 置换行，而 Q 的作用是按 q 置换行，所以由矩阵乘法的结合律，PQ 按 pq 置换行：
$$(PQ)X=P(QX).$$

因而 PQ 是 pq 相应的置换矩阵. 这就证明了(a). 我们把(b)的证明留作练习. ■

由(3.9)容易看出，置换矩阵的行列式为±1. 这个行列式称为置换的符号：

【4.9】
$$\operatorname{sign}p=\det P=\pm 1.$$

置换(4.2)的符号为+1，而任意对换的符号为−1[见(3.11ii)]. 根据其符号为−1 和+1 而称一个置换 p 为奇的和偶的.

现在回到任意 $n\times n$ 矩阵 A，利用行列式的线性性质(3.6)展开 $\det A$. 从第一行开始，应

26

用(3.6)，得到

$$\det A=\det\begin{bmatrix}a_{11}\,0\cdots 0\\ \text{——}R_2\text{——}\\ \vdots\\ \text{——}R_n\text{——}\end{bmatrix}+\det\begin{bmatrix}0\,a_{12}\,0\cdots 0\\ \text{——}R_2\text{——}\\ \vdots\\ \text{——}R_n\text{——}\end{bmatrix}+\cdots+\det\begin{bmatrix}0\cdots 0\,a_{1n}\\ \text{——}R_2\text{——}\\ \vdots\\ \text{——}R_n\text{——}\end{bmatrix}.$$

然后在第二行展开这些行列式，等等. 结束时，$\det A$ 表为许多项的和，其中每一项为一个在每一行仅留下一个元素的矩阵 M 的行列式：

$$M=\begin{bmatrix} & a_{1?} & \\ a_{2?} & & \\ & & a_{n?}\end{bmatrix}.$$

这些行列式中多数为零，因为其一整列为零. 于是一个 2×2 矩阵的行列式为四项之和：

$$\det\begin{bmatrix}a & b\\c & d\end{bmatrix}=\det\begin{bmatrix}a & 0\\c & d\end{bmatrix}+\det\begin{bmatrix}0 & b\\c & d\end{bmatrix}$$

$$=\det\begin{bmatrix}a & 0\\c & 0\end{bmatrix}+\det\begin{bmatrix}a & 0\\0 & d\end{bmatrix}+\det\begin{bmatrix}0 & b\\c & 0\end{bmatrix}+\det\begin{bmatrix}0 & b\\0 & d\end{bmatrix}.$$

由于第一项和第四项为零，于是

$$\det\begin{bmatrix}a & b\\c & d\end{bmatrix}=\det\begin{bmatrix}a & 0\\0 & d\end{bmatrix}+\det\begin{bmatrix}0 & b\\c & 0\end{bmatrix}.$$

事实上，没有一列为零的矩阵必在每一行和每一列留下一个非 0 元素 a_{ij}. 它们看起来很像置换矩阵 P，只不过是在 1 的位置用元素 a_{ij} 替代：

【4.10】
$$P=\sum_j e_{p(j)j},\quad M=\sum_j a_{p(j)j}e_{p(j)j}.$$

由行列式的线性性质(3.6)，

$$\det M=(a_{p(1)1}\cdots a_{p(n)n})(\det P)=(\operatorname{sign}p)(a_{p(1)1}\cdots a_{p(n)n}).$$

对每一个置换 p 有一个这样的项. 这就导出了公式

【4.11】
$$\det A=\sum_{\mathrm{perm}\,p}(\operatorname{sign}p)a_{p(1)1}\cdots a_{p(n)1},$$

27

其中和是在集合{**1**，…，***n***}的所有置换上取. 把这个公式写成转置的形式似乎看起来更好一些：

【4.12】
$$\det A=\sum_{\mathrm{perm}\,p}(\operatorname{sign}p)a_{1p(1)}\cdots a_{np(n)}.$$

这称为行列式的*完全展开*.

例如，3×3 矩阵的行列式的完全展开有六项：

【4.13】
$$\det\begin{bmatrix}a_{11} & a_{12} & a_{13}\\a_{21} & a_{22} & a_{23}\\a_{31} & a_{32} & a_{33}\end{bmatrix}$$

$$=a_{11}a_{22}a_{33}+a_{12}a_{23}a_{31}+a_{13}a_{21}a_{32}-a_{11}a_{23}a_{32}-a_{12}a_{21}a_{33}-a_{13}a_{22}a_{31}.$$

完全展开在理论上比在实际上更重要，因为项数太多，只有当 n 较小的时候才能用于计算. 其在理论上重要，是因为可以将它看成是以±1 为系数、有 n^2 个矩阵元素 a_{ij} 的多项式. 例如，假定每一矩阵元素 $a_{ij}=a_{ij}(t)$都是一个变量的可微函数，则 $\det A$ 也是 t 的可微函数，因为可微函数的和与积仍然是可微的.

第五节　克拉默法则

克拉默法则是用行列式给出线性方程组解的一组公式的统称. 要导出这些公式，需要对除第一列以外的其他列进行子式展开，还需要在行上展开.

【5.1】 *在第 j 列对子式展开：*

$$\det A=(-1)^{j+1}a_{1j}\det A_{1j}+(-1)^{j+2}a_{2j}\det A_{2j}+\cdots+(-1)^{j+n}a_{nj}\det A_{nj}.$$

【5.2】 *在第 i 行对子式展开：*

$$\det A=(-1)^{i+1}a_{i1}\det A_{i1}+(-1)^{i+2}a_{i2}\det A_{i2}+\cdots+(-1)^{i+n}a_{in}\det A_{in}.$$

在这些公式中，A_{ij}是矩阵(3.3)．项$(-1)^{i+j}$给出了依赖于矩阵中位置(i, j)的交错符号．(我

28

怀疑这种巧妙的记号是否有帮助，但这已成为习惯．)符号可由下图读出：

【5.3】

$$\begin{bmatrix} + & - & + & - & \cdots \\ - & + & & & \\ + & - & & & \\ \vdots & & & \ddots & \end{bmatrix}.$$

用下面两种方法之一可以证明(5.1)：

(a) 直接对(5.1)验证性质(3.5)～(3.7)并应用定理(3.14)．

(b) 交换(列 j)和(列 1)并应用(3.9′)及(3.19)．

我们省去这些验证．一旦证明了(5.1)，(5.2)可通过转置矩阵并应用(3.18)得到．

【5.4】定义 设 A 为 $n\times n$ 矩阵，A 的**伴随矩阵**是一个 $n\times n$ 矩阵，其(i, j)元素$(\mathrm{adj}A)_{ij}$为$(-1)^{i+j}\det A_{ji}=\alpha_{ji}$，这里 A_{ij} 是如(3.3)由 A 删去第 i 行和第 j 列后得到的矩阵：

$$(\mathrm{adj}A)=(\alpha_{ij})^t,$$

其中 $\alpha_{ij}=(-1)^{i+j}\det A_{ij}$．这样

【5.5】

$$\mathrm{adj}\begin{bmatrix} a & b \\ c & d \end{bmatrix}=\begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

而

【5.6】

$$\mathrm{adj}\begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{bmatrix}=\begin{bmatrix} 4 & 1 & -2 \\ -2 & 0 & 1 \\ -3 & -1 & 2 \end{bmatrix}^t=\begin{bmatrix} 4 & -2 & -3 \\ 1 & 0 & -1 \\ -2 & 1 & 2 \end{bmatrix}.$$

我们现在着手推导称为克拉默法则的公式．

【5.7】定理 设 $\delta=\det A$，则

$$(\mathrm{adj}A)\cdot A=\delta I,\quad A\cdot(\mathrm{adj}A)=\delta I.$$

注意，在这些方程中

$$\delta I=\begin{bmatrix} \delta & & \\ & \ddots & \\ & & \delta \end{bmatrix}.$$

29

【5.8】推论 设 A 的行列式 δ 不为零，则

$$A^{-1}=\frac{1}{\delta}(\mathrm{adj}A).$$

例如，2×2 矩阵$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$的逆为

$$\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

在(5.6)中计算伴随矩阵的 3×3 矩阵的行列式刚好为 1，对这个矩阵，有 $A^{-1}=\mathrm{adj}A$．

定理(5.7)的证明是很容易的．$(\mathrm{adj}A)\cdot A$ 的(i, j)元素为

【5.9】

$$(\mathrm{adj})_{i1}a_{1j}+\cdots+(\mathrm{adj})_{in}a_{nj}=\alpha_{1i}a_{1j}+\cdots+\alpha_{ni}a_{nj}.$$

如果 $i=j$，这是计算 δ 的公式(5.1)，恰好是我们需要的答案. 设 $i\neq j$. 考虑在矩阵 A 中用(列 j)代替(列 i)得到的矩阵 B. 这时，(列 j)在矩阵 B 中出现两次. 于是(5.9)为 B 在第 i 列对子式的展开. 但由(3.7′)及(3.19)，$\det B=0$. 故(5.9)为零，这正是要证明的. 定理(5.7)的第二个等式可以类似证明.

当 A 是 $n\times n$ 矩阵，且 $\det A\neq 0$ 时，公式(5.8)可用于求以紧凑形式写出的线性方程组 $AX=B$ 的解. 两边乘以 A^{-1}，得

【5.10】
$$X=A^{-1}B=\frac{1}{\delta}(\mathrm{adj}A)B,$$

其中 $\delta=\det A$，右边的积可以展开而得到公式

【5.11】
$$x_j=\frac{1}{\delta}(b_1\alpha_{1j}+\cdots+b_n\alpha_{nj}),$$

其中 $\alpha_{ij}=\pm\det A_{ij}$ 如上面所定义.

注意到(5.11)右边的主项 $b_1\alpha_{1j}+\cdots+b_n\alpha_{nj}$ 看起来就像行列式在第 j 列对子式展开，只不过是用 b_i 代替 a_{ij}. 加上这一事实，可以得到线性方程组解的另一个表达式. 下面用列向量 B 代替 A 的第 j 列构造一个新矩阵 M_j. 在第 j 列对子式展开得到

$$\det M_j=(b_1\alpha_{1j}+\cdots+b_n\alpha_{nj}).$$

这就给出了一个漂亮的公式

【5.12】
$$x_j=\frac{\det M_j}{\det A}.$$

由于某种原因，把线性方程组 $AX=B$ 的解写成这种形式是很普遍的，通常这种形式称为克拉默法则. 然而，这一表达式并没有简化计算. 要记住的是，(5.8)把矩阵的逆用其伴随矩阵表出，其他公式都由此表达式得到.

与行列式的完全展开(4.10)相比，公式(5.8)～(5.11)在理论上和实际上都非常有意义，因为 A^{-1} 和 X 的解答都具体表示为具有整系数的变量 $\{a_{ij}, b_i\}$ 的多项式的商. 例如，当 a_{ij} 和 b_i 都是 t 的函数时，解 x_i 也是.

一个表为展开形式的一般代数行列式
也许就像看似均匀的多种液体的混合物一样，由于沸点不同，
可以用分步蒸馏法加以分离.

James Joseph Sylvester

练　　习

第一节　基本运算

1. 矩阵 $\begin{bmatrix}1&2&5\\2&7&8\\0&9&4\end{bmatrix}$ 的元素 a_{21} 和 a_{23} 是什么？

2. 对于下列矩阵 A 和 B，计算积 AB 和 BA.

30

(a) $A=\begin{bmatrix}1 & 2 & 3\\ 3 & 3 & 1\end{bmatrix}$，$B=\begin{bmatrix}-8 & -4\\ 9 & 5\\ -3 & -2\end{bmatrix}$.

(b) $A=\begin{bmatrix}1 & 4\\ 1 & 2\end{bmatrix}$，$B=\begin{bmatrix}6 & -4\\ -3 & 2\end{bmatrix}$.

(c) $A=\begin{bmatrix}1\\ -1\\ 0\end{bmatrix}$，$B=[1\quad 2\quad 1]$.

3. 设 $A=(a_1,\ \cdots,\ a_n)$ 为行向量，而 $B=\begin{bmatrix}b_1\\ \vdots\\ b_n\end{bmatrix}$ 为列向量，求积 AB 和 BA.

4. 对下列矩阵乘积验证结合律：

$$\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}\begin{bmatrix}0 & 1 & 2\\ 1 & 1 & 3\end{bmatrix}\begin{bmatrix}1\\ 4\\ 3\end{bmatrix}.$$

31

注意这是一个自验证问题，你必须乘对了，否则结果出不来．若你需要练习更多矩阵乘积，可以以本题为模型．

5. 计算积 $\begin{bmatrix}1 & a\\ & 1\end{bmatrix}\begin{bmatrix}1 & b\\ & 1\end{bmatrix}$.

6. 计算 $\begin{bmatrix}1 & 1\\ & 1\end{bmatrix}^n$.

7. 找出 $\begin{bmatrix}1 & 1 & 1\\ & 1 & 1\\ & & 1\end{bmatrix}^n$ 的公式，并用归纳法证明．

8. 用分块乘法计算下列矩阵：

$$\left[\begin{array}{cc|cc}1 & 1 & 1 & 5\\ 0 & 1 & 0 & 1\\ \hline 1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\end{array}\right]\left[\begin{array}{cc|cc}1 & 2 & 1 & 0\\ 0 & 1 & 0 & 1\\ \hline 1 & 0 & 0 & 1\\ 0 & 1 & 1 & 3\end{array}\right],\quad \left[\begin{array}{c|cc}0 & 1 & 2\\ \hline 0 & 1 & 0\\ 3 & 0 & 1\end{array}\right]\left[\begin{array}{c|cc}1 & 2 & 3\\ \hline 4 & 2 & 3\\ 5 & 0 & 4\end{array}\right].$$

9. 对分块乘法证明(1.20)．

10. 设 A，B 为方阵．

(a) $(A+B)(A-B)=A^2-B^2$ 何时成立？

(b) 展开 $(A+B)^3$.

11. 设 D 是对角矩阵

$$\begin{bmatrix}d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n\end{bmatrix},$$

并设 $A=(a_{ij})$ 为任意 $n\times n$ 矩阵．

(a) 计算积 DA 和 AD.

(b) 计算两个对角矩阵的积．

(c) 对角矩阵何时可逆?

12. $n\times n$ 矩阵称为上三角的，如果对任意 $i>j$ 有 $a_{ij}=0$. 证明两个上三角矩阵之积是上三角矩阵.

13. 对下列每种情形，找出与所给矩阵交换的所有实 2×2 矩阵.

(a) $\begin{bmatrix}1&0\\0&0\end{bmatrix}$ (b) $\begin{bmatrix}0&1\\0&0\end{bmatrix}$ (c) $\begin{bmatrix}2&0\\0&6\end{bmatrix}$ (d) $\begin{bmatrix}1&3\\0&1\end{bmatrix}$ (e) $\begin{bmatrix}2&3\\0&6\end{bmatrix}$

14. 证明零矩阵的性质：$0+A=A$, $0A=0$ 和 $A0=0$.

15. 证明有一行为零的矩阵不可逆.

16. 方阵 A 如果满足条件：存在 $k>0$ 使 $A^k=0$，则称为是**幂零的**. 证明：如果 A 是幂零的，则 $I+A$ 可逆.

17. (a) 当

$$A=\begin{bmatrix}2&3\\1&2\\2&5\end{bmatrix}$$

时，找出无限多个矩阵 B 使 $BA=I_2$.

(b) 证明不存在矩阵 C 使 $AC=I_3$.

32

18. 仔细写出命题(1.18)的证明，利用结合律求积 $(AB)(B^{-1}A^{-1})$.

19. 方阵的迹是其对角元素的和：

$$\mathrm{tr}A=a_{11}+a_{22}+\cdots+a_{nn}.$$

(a) 证明 $\mathrm{tr}(A+B)=\mathrm{tr}A+\mathrm{tr}B$, $\mathrm{tr}AB=\mathrm{tr}BA$.

(b) 证明：若 B 可逆，则 $\mathrm{tr}A=\mathrm{tr}BAB^{-1}$.

20. 证明方程 $AB-BA=I$ 对 $n\times n$ 实元素矩阵没有解.

第二节 行约简

1. (a) 对(2.10)中矩阵 M 的约简，确定每一个变换所对应的初等矩阵.

(b) 计算这些初等矩阵的乘积 P，并验证 PM 的确是最终结果.

2. 设

$$A=\begin{bmatrix}1&2&1&1\\3&0&0&4\\1&-4&-2&-2\end{bmatrix},$$

而 B 取下列值：

(a) $\begin{bmatrix}0\\0\\0\end{bmatrix}$ (b) $\begin{bmatrix}1\\1\\0\end{bmatrix}$ (c) $\begin{bmatrix}0\\2\\2\end{bmatrix}$,

求方程组 $AX=B$ 的所有解.

3. 求方程 $x_1+x_2+2x_3-x_4=3$ 的所有解.

4. 求例(2.22)的行约简中所用到的初等矩阵，验证它们的积为 A^{-1}.

5. 求下列矩阵的逆：

$$\begin{bmatrix}1&\\&2\end{bmatrix},\begin{bmatrix}1&1\\&1\end{bmatrix},\begin{bmatrix}&1\\1&\end{bmatrix},\begin{bmatrix}3&5\\1&2\end{bmatrix},\begin{bmatrix}1&1\\&1\end{bmatrix}\begin{bmatrix}&1\\1&\end{bmatrix}\begin{bmatrix}3&5\\1&2\end{bmatrix}.$$

6. 画出矩阵 $A=\begin{bmatrix}2&-1\\2&3\end{bmatrix}$ 在平面 $\mathbb{R}^2$ 上乘积作用效果的草图.

7. 同时用行变换和列变换，矩阵可简化到什么程度?

8. (a) 计算积 $e_{ij}e_{k\ell}$.
   (b) 将单位矩阵写成矩阵单位的和.
   (c) 设 A 是任意 $n\times n$ 矩阵. 计算 $e_{ii}Ae_{jj}$.
   (d) 计算 $e_{ij}A$ 及 Ae_{ij}.
9. 对初等矩阵的作用证明(2.7).
10. 设 A 为方阵. 证明存在初等矩阵 $E_1,\cdots,E_k$ 使 $E_k\cdots E_1A$ 或为单位矩阵或其底行为零.
11. 证明每一个 2×2 可逆矩阵最多是四个初等矩阵的积.
12. 证明：如果 $n\times n$ 矩阵的积 AB 可逆，则其因子 A，B 皆可逆.
13. 一个矩阵 A 称为对称的，如果 $A=A^t$. 证明对任意矩阵 A，矩阵 AA^t 为对称矩阵，如果 A 为方阵，则 $A+A^t$ 为对称矩阵.

33

14. (a) 证明 $(AB)^t=B^tA^t$ 及 $A^{tt}=A$.
   (b) 证明：如果 A 可逆，则 $(A^{-1})^t=(A^t)^{-1}$.
15. 证明可逆对称矩阵的逆也是对称的.
16. 设 A 和 B 为对称的 $n\times n$ 矩阵. 证明积 AB 是对称的当且仅当 $AB=BA$.
17. 设 A 是一个 $n\times n$ 矩阵. 证明算子"用 A 左乘"在下列意义下确定 A：若对任意列向量 X 有 $AX=BX$，则 $A=B$.
18. 设 A，B 是实元素矩阵，考虑任意线性方程组 $AX=B$.
   (a) 证明：如果线性方程组 $AX=B$ 的解多于一个，则它有无穷多个解.
   (b) 证明：如果它有复数解，则它也有实解.

*19. 证明由矩阵 A 通过行约简得到的行阶梯矩阵由 A 唯一确定.

第三节　行列式

1. 求下列行列式的值.

$$\text{(a)}\begin{bmatrix}1 & i\\ 2-i & 3\end{bmatrix}\quad \text{(b)}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\quad \text{(c)}\begin{bmatrix}2 & 0 & 1\\ 0 & 1 & 0\\ 1 & 0 & 2\end{bmatrix}\quad \text{(d)}\begin{bmatrix}1 & 0 & 0 & 0\\ 5 & 2 & 0 & 0\\ 8 & 6 & 3 & 0\\ 0 & 9 & 7 & 4\end{bmatrix}\quad \text{(e)}\begin{bmatrix}1 & 4 & 1 & 3\\ 2 & 3 & 5 & 0\\ 4 & 1 & 0 & 0\\ 2 & 0 & 0 & 0\end{bmatrix}$$

2. 证明 $\det\begin{bmatrix}1 & 2 & 5 & 6\\ 3 & 1 & 7 & 7\\ 0 & 0 & 2 & 3\\ 4 & 2 & 1 & 5\end{bmatrix}=-\det\begin{bmatrix}2 & 1 & 5 & 1\\ 1 & 3 & 7 & 0\\ 0 & 0 & 2 & 1\\ 2 & 4 & 1 & 4\end{bmatrix}$.

3. 对矩阵 $A=\begin{bmatrix}2 & 3\\ 1 & 4\end{bmatrix}$，$B=\begin{bmatrix}1 & 1\\ 5 & -2\end{bmatrix}$，验证规则 $\det(AB)=(\det A)(\det B)$. 注意这是一个自验证问题，可以以此作为模型练习计算行列式.

4. 对 n 用数学归纳法计算下列 $n\times n$ 矩阵的行列式.

$$\text{(a)}\begin{bmatrix} & & & 1\\ & & 1 & \\ & \iddots & & \\ 1 & & & \end{bmatrix},\quad \text{(b)}\begin{bmatrix}2 & -1 & & & & \\ -1 & 2 & -1 & & & \\ & -1 & 2 & -1 & & \\ & & -1 & \ddots & & \\ & & & & 2 & -1\\ & & & & -1 & 2\end{bmatrix}$$

5. 计算 $\det\begin{bmatrix}1 & 2 & 3 & \cdots & n\\ 2 & 2 & 3 & & \vdots\\ 3 & 3 & 3 & & \vdots\\ \vdots & & & \ddots & \vdots\\ n & & & \cdots & n\end{bmatrix}$.

34

*6. 计算 $\det\begin{bmatrix}2 & 1 & & & & & & \\ 1 & 2 & 1 & & & & & \\ & 1 & 2 & 1 & & & & \\ & & 1 & 2 & 1 & & & \\ & & & 1 & 2 & 1 & & 1\\ & & & & 1 & 2 & 1 & \\ & & & & & 1 & 2 & \\ & & & & 1 & & & 2\end{bmatrix}$.

7. 证明如(3.6)的断言，行列式关于矩阵的行是线性的.

8. 设 A 是一个 $n\times n$ 矩阵. $\det(-A)$是什么？

9. 证明 $\det A^t=\det A$.

10. 由性质(3.5)、(3.6)、(3.7)、(3.9)推导公式 $\det\begin{bmatrix}a & b\\ c & d\end{bmatrix}=ad-bc$.

11. 设 A，B 为方阵，证明 $\det(AB)=\det(BA)$.

12. 若 A 和 D 为方阵，证明 $\det\begin{bmatrix}A & B\\ 0 & D\end{bmatrix}=(\det A)(\det D)$.

*13. 设 $M=\begin{bmatrix}A & B\\ C & D\end{bmatrix}$为一个 $2n\times 2n$ 矩阵，其中每一块为一个 $n\times n$ 矩阵. 假设 A 可逆且 $AC=CA$. 证明$\det M=\det(AD-CB)$. 举例说明当 $AC\neq CA$ 时这一公式不成立.

第四节　置换矩阵

1. 考虑由 $1\rightsquigarrow 3$，$2\rightsquigarrow 1$，$3\rightsquigarrow 4$，$4\rightsquigarrow 2$ 定义的置换 p.

   (a) 求相应的置换矩阵 P.

   (b) 将 p 写为对换的积，并求对应的矩阵积.

   (c) 计算 p 的符号.

2. 证明每一个置换矩阵是对换矩阵的积.

3. 证明每行仅有单独一个 1 并且每列也仅有单独一个 1，而其他元素皆为零的矩阵为置换矩阵.

4. 设 p 为置换，证明 $\operatorname{sign}p=\operatorname{sign}p^{-1}$.

5. 证明置换矩阵 P 的转置是它的逆.

6. 与置换 $i\rightsquigarrow n-i$ 相应的置换矩阵是什么？

7. (a) 3×3 矩阵的行列式的完全展开共有六项，每项带有正负号，并且是三个元素之积，它们是什么？

   (b) 用完全展开式求下列矩阵的行列式，并用其他方法验证你的结果：

$$\begin{bmatrix}1 & 1 & 2\\ 2 & 4 & 2\\ 0 & 2 & 1\end{bmatrix},\begin{bmatrix}4 & -1 & 1\\ 1 & 1 & -2\\ 1 & -1 & 1\end{bmatrix},\begin{bmatrix}a & b & c\\ 1 & 0 & 1\\ 1 & 1 & 1\end{bmatrix}.$$

8. 通过验证规则(3.5)～(3.7)证明完全展开(4.12)定义了行列式.

35

9. 证明公式(4.11)和(4.12)定义了同一个数.

第五节 克拉默法则

1. 设$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$是行列式为1的矩阵. A^{-1}是什么?

2. (自验证)求矩阵$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 & 2 \\ 2 & 4 & 2 \\ 0 & 2 & 1 \end{bmatrix}$, $\begin{bmatrix} 4 & -1 & 1 \\ 1 & 1 & -2 \\ 1 & -1 & 1 \end{bmatrix}$和$\begin{bmatrix} a & b & c \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$的伴随矩阵，并对它们验证定理(5.7).

3. 设A是元素a_{ij}为整数的$n \times n$矩阵. 证明A^{-1}为整数元素的充分必要条件是$\det A = \pm 1$.

4. 证明矩阵在一行关于子式展开定义了行列式函数.

杂题

1. 用尽可能少的初等矩阵的积表出矩阵$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$. 证明你的表达式是最短的.

2. 将复数用2×2实矩阵表出，它与加法和乘法都相容. 从求矩阵方程$A^2 = -I$的一个好的解入手.

3. (范德蒙德行列式)

   (a) 证明$\det \begin{bmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{bmatrix} = (b-a)(c-a)(c-b)$.

   *(b) 通过行变换巧妙地删去第一列，对$n \times n$矩阵证明类似的公式.

*4. 考虑m个有n个未知量的线性方程构成的一般线性方程组$AX = B$. 若系数矩阵A有左逆A'，即满足$A'A = I_n$的矩阵，则可如下解方程组：

$$AX = B$$
$$A'AX = A'B$$
$$X = A'B.$$

如果我们想要反过来验证，会遇到麻烦：

$$X = A'B$$
$$AX = AA'B$$
$$AX \stackrel{?}{=} B.$$

36

我们似乎需要A'为A的右逆：$AA' = I_m$，但这是不对的. 给出解释. (提示：举出一些例子.)

5. (a) 设A是2×2实矩阵，并设A_1, A_2为其行. 设P是顶点为0, A_1, A_2, $A_1 + A_2$的平行四边形. 通过比较初等行变换对面积和对$\det A$作用的效果，证明P的面积是行列式$\det A$的绝对值.

   *(b) 对$n \times n$矩阵证明类似的结果.

*6. 大多数可逆矩阵可以写成一个下三角矩阵L和一个上三角矩阵U的积：$A = LU$，而且其中U的对角元素皆是1.

   (a) 证明唯一性，即证明A最多有一种方式写成这样的积.

   (b) 说明当A给定时，如何计算L和U.

   (c) 证明每一可逆矩阵可以写为LPU，其中L, U如上而P是置换矩阵.

7. 考虑n个有n个未知量的线性方程构成的线性方程组：$AX = B$，其中A, B的元素皆为整数. 证明或否定下列断言.

   (a) 若$\det A \neq 0$，方程组具有有理解.

   (b) 若方程组具有有理解，则它也有整数解.

37

*8. 设A, B分别为$m \times n$和$n \times m$矩阵. 证明$I_m - AB$是可逆的当且仅当$I_n - BA$是可逆的.

第二章 群

在数学中没有几个概念比合成法则更加本原.

Nicolas Bourbaki

第一节 群的定义

本章我们学习最重要的代数概念之一——群. 群是在其中定义了一个合成法则，使得每一个元素都有逆的集合. 精确的定义将在下面(1.10)给出. 例如，非零实数集合关于乘法构成一个群$\mathbb{R}^{\times}$，而所有实数集合关于加法构成一个群$\mathbb{R}^{+}$. 可逆$n\times n$矩阵的集合，称为一般线性群，是一个非常重要的例子，其合成法则为矩阵乘法. 我们在后面还会看到许多其他例子.

集合S上的一个**合成法则**，是指由S的一对元素a，b合起来而得到S中的另一个元素(比如说p)的法则. 这个概念的原始模型是实数的加法和乘法. 从形式上讲，合成法则是S上的一个在S中取值的两个变量的函数，或者说它是一个映射

$$S\times S\longrightarrow S$$

$$a,b \rightsquigarrow p.$$

这里，$S\times S$像通常一样表示集合S的元素对(a, b)构成的积集.

对于合成法则，函数记号$p=f(a, b)$用起来不太方便. 通常用类似加法和乘法的记号来表示在一对元素(a, b)上应用合成法则所得到的元素：

$$p = ab, a\times b, a\circ b, a+b, \text{等等},$$

根据所讨论的法则选择适当的记号. 根据所选的记号，我们把元素p称为a与b的积或和.

合成法则的第一个例子，也是两个主要例子之一，是$n\times n$矩阵集S上的矩阵乘法.

我们最经常使用的记号是乘积记号ab. 用乘积记号证明的所有结论皆可用于其他记号，如加号，这是因为所改变的只有记号.

重要的是要注意乘积记号ab是S中某个元素的记号. 也就是说，它是在称为a和b的元素上应用给定的合成法则得到的元素. 这样，如果合成法则是矩阵乘积，$a=\begin{bmatrix}1 & 3\\ 0 & 2\end{bmatrix}$而$b=\begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix}$，则$ab$表示矩阵$\begin{bmatrix}7 & 3\\ 4 & 2\end{bmatrix}$. 一旦$ab$取值以后，元素$a$，$b$就不可能重新由它得到.

现在考虑写成乘法形式ab的一个合成法则. 如果对所有S中的a，b，c，法则

【1.1】
$$(ab)c = a(bc) \quad \text{（结合律）}$$

成立，则称之为**结合的**. 如果对所有S中的a，b，法则

【1.2】
$$ab = ba \quad \text{（交换律）}$$

成立，则称之为**交换的**. 上述矩阵乘法的例子是结合的但非交换的.

一般来说，在讨论群时，我们将使用乘法记号. 习惯上将记号$a+b$留给交换的合成法则，即对所有a，b满足$a+b=b+a$的合成法则. 乘法记号对满足或不满足交换律并没有特别的

意义.

结合律在加法记号下为$(a+b)+c=a+(b+c)$，在函数记号下为

$$f(f(a,b),c)=f(a,f(b,c)).$$

这一难看的公式表明了函数记号对于代数运算来说使用不方便这一事实.

结合律比交换律更为基本，其原因之一是我们合成法则的第二个例子，也就是函数的合成，是结合的. 设 T 为集合，g，f 是 T 到 T 的函数(或映射). 令 $g\circ f$ 表示合成映射 $t \rightsquigarrow g(f(t))$. 法则

$$g,f \rightsquigarrow g\circ f$$

是所有映射 $T\longrightarrow T$ 的集合 $S=\mathrm{Maps}(T,\ T)$上的合成法则.

与矩阵乘法一样，函数的合成也是一个结合的合成法则. 这是因为，若 f，g，h 是 T 到其自身的三个映射，则$(h\circ g)\circ f=h\circ(g\circ f)$：

$$T\xrightarrow{f}T\xrightarrow{g}T\xrightarrow{h}T.$$

（上方弧线标 $h\circ g$，下方弧线标 $g\circ f$）

39

这是显然的，因为两边的合成映射都使 $t\rightsquigarrow h(g(f(t)))$.

最简单的例子是 T 为两个元素的集合$\{a,\ b\}$. 这时有四个映射 $T\longrightarrow T$：

i：恒等映射，由 $i(a)=a$，$i(b)=b$ 定义；

τ：对换，由$\tau(a)=b$，$\tau(b)=a$ 定义；

α：常映射，$\alpha(a)=\alpha(b)=a$；

β：常映射，$\beta(a)=\beta(b)=b$.

S 的合成法则由下面的乘法表给出：

【1.3】

	i	τ	α	β
i	i	τ	α	β
τ	τ	i	β	α
α	α	α	α	α
β	β	β	β	β

它应理解为

$$\begin{array}{c|ccc} & \cdots & v & \cdots \\ \vdots & & \vdots & \\ u & \cdots & u\circ v & \cdots \\ \vdots & & \vdots & \end{array}$$

于是$\tau\circ\alpha=\beta$而$\alpha\circ\tau=\alpha$. 函数的合成不是交换的.

回到一般的合成法则，如果我们想定义集合中 n 个元素串的乘积：

$$a_1a_2\cdots a_n=?$$

使用给定的法则有多种方法来完成，法则告诉我们如何乘两个元. 例如，可先用法则求出 a_1a_2，然后用这个元素与 a_3 相乘，等等：

$$((a_1a_2)a_3)a_4\cdots.$$

当 $n=4$ 时，还有四种其他方式来组合这些相同的元素，比如 $(a_1a_2)(a_3a_4)$ 就是其中之一. 由数学归纳法可以证明，如果这个法则是结合的，则所有这样的乘积都相等. 这使我们可以讨论任意元素串的积.

【1.4】命题 设给定集合 S 上一个结合的合成法则. 对任意正整数 n，存在唯一的方法定义 S 中 n 个元素 a_1，…，a_n 的乘积(暂记作 $[a_1\cdots a_n]$)，使之满足下列条件：

(i) 一个元的积 $[a_1]$ 是该元素本身.

(ii) 两个元的积 $[a_1a_2]$ 由合成法则给定.

(iii) 对 1 和 n 之间的任意整数 i，有 $[a_1\cdots a_n]=[a_1\cdots a_i][a_{i+1}\cdots a_n]$.

(iii) 右边的意思是先作两个积 $[a_1\cdots a_i]$ 和 $[a_{i+1}\cdots a_n]$，再用给定的合成法则把它们相乘得到结果.

40

证明 对 n 作数学归纳. 当 $n\leqslant 2$ 时积由(i)和(ii)定义，且当 $n=2$ 时满足(iii). 设当 $r\leqslant n-1$ 时，我们已知如何定义 r 个元的积，且这个积是唯一的满足(iii)的积. 这时用法则

$$[a_1\cdots a_n]=[a_1\cdots a_{n-1}][a_n]$$

定义 n 个元的积，这里右边的项都是已经定义了的. 如果存在满足(iii)的积，则这个公式正好给出了这个积，因为当 $i=n-1$ 时它就是(iii). 因此，如果积存在，则它必是唯一的. 我们需对 $i<n-1$ 证明(iii)：

$$\begin{aligned}[a_1\cdots a_n]&=[a_1\cdots a_{n-1}][a_n] && \text{(由定义)}\\ &=([a_1\cdots a_i][a_{i+1}\cdots a_{n-1}])[a_n] && \text{(归纳假设)}\\ &=[a_1\cdots a_i]([a_{i+1}\cdots a_{n-1}][a_n]) && \text{(结合律)}\\ &=[a_1\cdots a_i][a_{i+1}\cdots a_n] && \text{(归纳假设)}\end{aligned}$$

这就完成了证明. 从现在起，我们将去掉括号而将乘积记为 $a_1\cdots a_n$. ■

合成法则的单位元是 S 中具有以下性质的元素 e：

【1.5】 $$\text{对所有 } a\in S, ea=a \quad \text{且} \quad ae=a.$$

单位元最多只有一个. 因为若有两个单位元 e，e'，则由于 e 是单位元，$ee'=e'$，又 e' 也是单位元，$ee'=e$. 从而 $e=e'$.

在我们的两个例子中，矩阵乘法和函数的合成都有单位元. 在 $n\times n$ 矩阵中它是单位矩阵 I，而在 Maps(T, T) 中，它是将 T 中的每一个元素映到其自身的恒等映射.

通常，当合成法则写作乘法形式时，单位元记作 1，而写作加法形式时记作 0. 这些元素与数 1 和 0 不一定有什么关系，但都具有合成法则单位元的性质.

假设合成法则有单位元，并用符号 1 来表示. 元素 $a\in S$ 称为可逆的，如果有另一个元素 b 使

$$ab=1 \quad \text{且} \quad ba=1.$$

41

像矩阵乘法一样[第一章(1.17)]，由结合律可以得到，逆元素如果存在，则是唯一的. 将它记为 a^{-1}：

$$aa^{-1}=a^{-1}a=1.$$

逆以相反的顺序相乘：

【1.6】 $$(ab)^{-1}=b^{-1}a^{-1}.$$

其证明与矩阵的情形相同[第一章(1.18)].

对于结合的合成法则，可使用幂记号

【1.7】
$$a^n = \underbrace{a\cdots a}_{n\text{个}} \quad (n \geqslant 1)$$
$$a^0 = 1 \qquad \text{如果单位元存在}$$
$$a^{-n} = a^{-1}\cdots a^{-1} \qquad \text{如果 } a \text{ 可逆}.$$
通常的幂运算法则都成立：

【1.8】
$$a^{r+s} = a^r a^s \quad \text{以及} \quad (a^r)^s = a^{rs}.$$
除非合成法则是交换的，否则最好不要引入分式记号

【1.9】
$$\frac{b}{a},$$
因为不知道这个分式记号所指的是 ba^{-1} 还是 $a^{-1}b$，而二者可以是不同的.

当合成法则写作加法形式时，将逆记为 $-a$，而幂记号 a^n 用 $na = a + \cdots + a$ 代替，这些与实数加法是一样的.

【1.10】定义 *群是一个具有结合的合成法则的集合 G，它有单位元，且 G 的每一个元素有逆.*

通常用同一个符号表示群与其元素的集合.

*阿贝尔群*是合成法则交换的群. 对阿贝尔群常用加法记号. 下面是一些阿贝尔群的例子：

【1.11】

$\mathbb{Z}^+$：整数，加法

$\mathbb{R}^+$：实数，加法

$\mathbb{R}^\times$：非零实数，乘法

$\mathbb{C}^+$，$\mathbb{C}^\times$：类似的群，用复数集$\mathbb{C}$代替实数$\mathbb{R}$.

下面是群的一个重要性质.

42

【1.12】命题 *消去律：设 a，b，c 是群 G 的元素. 如果 $ab=ac$，则 $b=c$. 如果 $ba=ca$，则 $b=c$.*

证明 $ab=ac$ 的两边左乘 a^{-1} 得到：$b=a^{-1}ab=a^{-1}ac=c$. ■

这个证明中用 a^{-1} 左乘不是一个技巧，而是很本质的. 若元素 a 不可逆，则消去律不一定成立. 例如，$0\cdot 1=0\cdot 2$，或者
$$\begin{bmatrix} 1 & \\ & \end{bmatrix}\begin{bmatrix} 1 & \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \\ & \end{bmatrix}\begin{bmatrix} 1 & \\ & 3 \end{bmatrix}.$$

两个最基本的群的例子由前面讨论过的合成法则——矩阵乘法和函数的合成——通过把不可逆的元素去掉而得到. 如我们在第一章所提到的，$n\times n$ *一般线性群*是由所有 $n\times n$ 可逆矩阵构成的群. 将它记为

【1.13】
$$GL_n = \{\text{满足 } \det A \neq 0 \text{ 的 } n\times n \text{ 矩阵 } A\}.$$
如果我们希望指出考虑的是实数矩阵还是复数矩阵，则把它们相应地记为
$$GL_n(\mathbb{R}) \quad \text{或} \quad GL_n(\mathbb{C}).$$

在函数集 $S=\mathrm{Maps}(T,T)$中，映射 $f: T \longrightarrow T$ 有逆当且仅当它是一一映射. 这样的映射也称为 T 的一个*置换*. 置换的集合构成一个群. 在例(1.3)中，可逆元素为 i 和 τ，它们构成一个有两个元素的群. 这两个元素就是集合$\{a, b\}$的所有置换.

整数 1 到 n 的集合$\{\mathbf{1},\mathbf{2},\cdots,\boldsymbol{n}\}$的置换群称为*对称群*，记作 S_n：

【1.14】
$$S_n = \{\mathbf{1},\cdots,\boldsymbol{n}\} \text{ 的置换群}.$$

因为 n 元集合共有 $n!$ 个置换，所以这个群有 $n!$ 个元.（我们说群的阶为 $n!$.）对称群 S_2 由两个元素 i 和 τ 构成，其中 i 表示恒等置换，而 τ 表示(1.3)中使 **1**，**2** 互换的对换．群的法则，即函数的合成，由 i 是单位元和关系 $\tau\tau=\tau^2=i$ 刻画.

S_n 的构造随着 n 的增加而迅速地变复杂，但在 $n=3$ 情形，很容易作出来．对称群 S_3 含有六个元素．对我们来说，这是一个重要的例子，因为它是合成法则非交换的最小群．为了刻画这个群，我们取两个特殊的置换 x，y，所有其他的置换可用它们表出．取 x 为指标的循环置换．它由第一章中的矩阵(4.3)表示：

43

【1.15】
$$x=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}.$$

对于 y，我们取互换 **1**，**2** 而保持 **3** 不变的对换：

【1.16】
$$y=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}.$$

集合{**1**，**2**，**3**}的六个置换为

【1.17】
$$\{1,x,x^2,y,xy,x^2y\}=\{x^iy^j\mid 0\leqslant i\leqslant 2,0\leqslant j\leqslant 1\},$$

其中 1 是恒等置换．可通过计算乘积来验证这一点.

法则

【1.18】
$$x^3=1,\quad y^2=1,\quad yx=x^2y$$

也可直接验证．对 S_3 的计算有它们就足够了．不断应用上面的法则，x，y 以及其逆的任意积，例如 $x^{-1}y^3x^2y$，都可以写为 x^iy^j 的形式，其中 $0\leqslant i\leqslant 2$，而 $0\leqslant j\leqslant 1$．为此，用最后一个关系把所有出现的 y 移到右边，而用前面两个关系使其幂变到指定范围：

$$x^{-1}y^3x^2y=x^2yx^2y=x^2(yx)xy=x^2x^2yxy=\cdots=x^6y^2=1.$$

用这些法则，可以写出 S_3 的完全的乘法表．因此，这些法则称为群的*定义关系*，我们会在第六章正式学习这一概念.

注意，因为 $yx\neq xy$，所以在 S_3 中交换律不成立.

第二节 子　群

一般线性群和对称群如此重要的一个原因，是许多其他群都作为子群包含在它们之中．群 G 的子集 H 称为一个*子群*，如果它具有下列性质：

【2.1】

(a) *封闭性*：若 $a\in H$ 并且 $b\in H$，则 $ab\in H$.

(b) *单位元*：$1\in H$.

(c) *逆元*：若 $a\in H$，则 $a^{-1}\in H$.

对这些条件解释如下：第一个条件(a)告诉我们可以用 G 上的合成法则在 H 上定义一个合成法则，称之为*诱导的合成法则*．第二个条件(b)和第三个条件(c)，指出 H 关于这个诱导法

则构成一个群. 注意,(2.1)提到了群定义中除了结合律的所有要点. 因为结合律自动地由 G 转移到 H,我们不需要再提及它.

44

每个群都有两个明显的子群:整个群和由单独一个单位元构成的子群$\{1\}$. 一个子群如果不是这两个子群之一,称为真子群.

下面是两个子群的例子.

【2.2】例

(a) 2×2 可逆上三角矩阵

$$\begin{bmatrix} a & b \\ & d \end{bmatrix} \quad (a,d\neq 0)$$

的集合 T 是一般线性群 $GL_2(\mathbb{R})$ 的子群.

(b) 绝对值为 1 的复数的集合——复平面的单位圆上点的集合——是 $\mathbb{C}^{\times}$ 的一个子群.

作为更多的例子,我们将确定整数加法群 $\mathbb{Z}^{+}$ 的子群. 记由给定整数 b 的倍数构成的 $\mathbb{Z}$ 的子集为 $b\mathbb{Z}$:

【2.3】
$$b\mathbb{Z}=\{n\in\mathbb{Z}\mid 存在\ k\in\mathbb{Z},使\ n=bk\}.$$

【2.4】命题 对任意整数 b,子集 $b\mathbb{Z}$ 是 $\mathbb{Z}^{+}$ 的子群. 而且 $\mathbb{Z}^{+}$ 的每一子群 H 必有 $H=b\mathbb{Z}$ 的形式,这里 b 是一个整数.

证明 我们将 $b\mathbb{Z}$ 是子群的验证留作练习,而证明每一个子群都有这种形式. 设 H 是 $\mathbb{Z}^{+}$ 的一个子群. 记住 $\mathbb{Z}^{+}$ 的合成法则是加法,单位元是 0,而 a 的逆是 $-a$. 于是子群公理为

(i) 若 $a\in H$ 且 $b\in H$,则 $a+b\in H$.

(ii) $0\in H$.

(iii) 若 $a\in H$,则 $-a\in H$.

由公理(ii),$0\in H$. 若 0 是 H 中仅有的元,则 $H=0\mathbb{Z}$,因而对这一情形结论成立. 否则,H 中必有一正整数. 这是因为,令 $a\in H$ 是任意非零元素. 如果 a 为负数,则 $-a$ 为正数,而根据公理(iii) $-a$ 在 H 中. 取 b 为 H 中的最小正整数,我们断言 $H=b\mathbb{Z}$. 我们先证 $b\mathbb{Z}\subset H$,即对任意整数 k,$bk\in H$. 若 k 是正整数,则 $bk=b+\cdots+b$(k 项). 由公理(i)及数学归纳法知它属于 H. 由公理(iii),$b(-k)=-bk\in H$. 最后,由公理(ii),$b0=0\in H$.

接下来证明 $H\subset b\mathbb{Z}$,即任意元素 $n\in H$ 都是 b 的整数倍. 用带余除法,记 $n=bq+r$,其中 q,r 都是整数且余数 r 的取值范围为 $0\leqslant r<b$. 则 n 与 bq 都属于 H,于是,由公理(iii)和(i)知 $r=n-bq$ 亦属于 H. 由我们的选择,b 是 H 中的最小正整数,而 $0\leqslant r<b$. 从而 $r=0$,并且 $n=bq\in b\mathbb{Z}$,这正是要证明的. ■

45

子群 $b\mathbb{Z}$ 的元素可以刻画为能被 b 整除的所有整数. 这一刻画导致命题(2.3)在两个整数 a,b 生成的子群上的一个惊人的应用. 设 a 和 b 都非零. 集合

【2.5】
$$a\mathbb{Z}+b\mathbb{Z}=\{n\in\mathbb{Z}\mid n=ar+bs,r,s\ 是任意整数\}$$

是 $\mathbb{Z}^{+}$ 的子群. 它称为由 a 和 b 生成的子群,这是因为它是同时包含这两个元素的最小的子群. 命题(2.3)告诉我们存在某个整数 d,使这个子群具有 $d\mathbb{Z}$ 的形式,从而它是能被 d 整除的整数集合. 由于下面命题解释的原因,生成元 d 称为 a 与 b 的最大公因数.

【2.6】命题 设 a,b 为整数,不全为零,并设 d 是生成子群 $a\mathbb{Z}+b\mathbb{Z}$ 的正整数. 则有

(a) 存在整数 r 和 s,使 d 可以写为 $d=ar+bs$ 的形式.

(b) d 整除 a 与 b.

(c) 若整数 e 整除 a 和 b，则 e 整除 d.

证明 第一个断言(a)是 d 属于 $a\mathbb{Z}+b\mathbb{Z}$ 的另一种说法. 其次，注意到 a，b 都在子群 $d\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$ 中，因而 d 整除 a 与 b. 最后，若 e 是整除 a 和 b 的整数，则 a，b 皆属于 $e\mathbb{Z}$，这样，任意整数 $n=ar+bs$ 亦属于 $e\mathbb{Z}$. 由假设，d 具有这样的形式，故 e 整除 d. ■

给定两个整数 a，b，求其最大公因数的方法之一是将它们都分解成素数的积，然后取它们的公共因子. 于是 $36=2\cdot2\cdot3\cdot3$ 和 $60=2\cdot2\cdot3\cdot5$ 的最大公因数是 $12=2\cdot2\cdot3$. 性质(2.6)的(b)和(c)是容易验证的. 但如果没有命题(2.4)，用这种方法得到的整数具有 $ar+bs$ 的形式这一事实是看不出来的.（在我们的例子中，$12=36\cdot2-60\cdot1$.）我们将在第十一章讨论这一事实在算术中的应用.

现在看一个重要的抽象子群的例子，即由 G 中任意一个元素 x 生成的循环子群. 我们用乘法的记号. 由 x 生成的循环子群 H 是 x 的所有幂的集合：

【2.7】
$$H=\{\cdots,x^{-2},x^{-1},1,x,x^2,\cdots\}.$$

它是 G 的一个子群——包含 x 的最小子群. 但要想正确地解释(2.7)，必须记住 x^n 是 G 中某个元素的记号. 在我们所列的元素中会有重复. 例如，若 $x=1$，则我们所列的元素全都为 1. 要区分两种情况：x 的幂都是互不相同的，或不是互不相同的. 在第一种情形，群 H 称为无限循环群.

46

在第二种情形，假设有两个幂是相同的，比如说，存在 $n>m$ 使 $x^n=x^m$. 则 $x^{n-m}=1$[消去律(1.12)]，从而 x 有等于 1 的幂.

【2.8】引理 满足条件 $x^n=1$ 的整数 n 的集合 S 是 $\mathbb{Z}^+$ 的子群.

证明 若 $x^m=1$ 且 $x^n=1$，则亦有 $x^{m+n}=x^mx^n=1$. 这证明若 m，$n\in S$，则 $m+n\in S$. 于是子群公理(i)成立. 因为 $x^0=1$，子群公理(ii)也成立. 最后，若 $x^n=1$，则 $x^{-n}=x^nx^{-n}=x^0=1$. 从而，如果 $n\in S$ 则 $-n\in S$. ■

由引理(2.8)和命题(2.4)可得 $S=m\mathbb{Z}$，其中 m 是使 $x^m=1$ 的最小正整数. m 个元素 1，x，$\cdots$，x^{m-1} 互不相同.（若有 $0\leqslant i<j<m$ 使 $x^i=x^j$，则 $x^{j-i}=1$. 但 $j-i<m$，因此这是不可能的.）此外，任意幂 x^n 等于其中的一个：用带余除法，可记 $n=mq+r$，其中余数 r 小于 m. 于是 $x^n=(x^m)^qx^r=x^r$. 这样 H 由下列 m 个元素构成：

【2.9】
$$H=\{1,x,\cdots,x^{m-1}\},\text{这些幂互不相同,并且 } x^m=1.$$

这样的群称为 m 阶循环群.

群 G 的阶是其元素的个数. 阶常被记为

【2.10】
$$|G|=G\text{ 的元素个数}.$$

当然，阶可以是无限的.

如果群 G 的一个元生成的循环群的阶为 m，则称这个元的阶为 m(可能无限). 这表明 m 是使得 $x^m=1$ 的最小整数，或者当阶为无限大时，对所有的 $m\neq0$ 都有 $x^m\neq1$.

例如，在 $GL_2(\mathbb{R})$ 中矩阵 $\begin{bmatrix}1&1\\-1&0\end{bmatrix}$ 是 6 阶元素，于是它生成的循环子群的阶是 6. 另一方面，由于

$$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}^n = \begin{bmatrix}1 & n\\0 & 1\end{bmatrix},$$

故矩阵$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$有无限阶.

我们也会讲到群 G 中*由子集 U 生成的子群*. 这是指 G 中包含 U 的最小子群，它由 G 中所有可以表成 U 的元素和它们的逆的串的乘积的元素构成. 特别地，若 G 中的元素都可表成这样的积，则称 G 的子集 U *生成* G. 例如在(1.17)中，我们看到子集 $U=\{x, y\}$ 生成对称群 S_3. 第一章的命题(2.18)指出初等矩阵生成 GL_n.

47

克莱因四元数群 V 是最简单的非循环群. 它将以多种形式出现. 例如，它可以用由四个矩阵

【2.11】
$$\begin{bmatrix}\pm 1 & \\ & \pm 1\end{bmatrix}$$

组成的群实现. 任意两个不是单位元的元素生成 V.

四元数群 H 是 $GL_2(\mathbb{C})$中非循环的小子群的例子. 它由八个矩阵

【2.12】
$$H = \{\pm \mathbf{1}, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}\},$$

构成，其中

$$\mathbf{1} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \quad \boldsymbol{i} = \begin{bmatrix}\mathrm{i} & 0\\0 & -\mathrm{i}\end{bmatrix}, \quad \boldsymbol{j} = \begin{bmatrix}0 & 1\\-1 & 0\end{bmatrix}, \quad \boldsymbol{k} = \begin{bmatrix}0 & \mathrm{i}\\ \mathrm{i} & 0\end{bmatrix}.$$

元素 $\boldsymbol{i}$，$\boldsymbol{j}$ 生成 H，通过计算可得下列公式：

【2.13】
$$\boldsymbol{i}^4 = \mathbf{1}, \quad \boldsymbol{i}^2 = \boldsymbol{j}^2, \quad \boldsymbol{ji} = \boldsymbol{i}^3\boldsymbol{j}.$$

这些积确定了 H 的乘法表.

第三节　同　构

设 G 和 G' 为两个群. 如果 G 的结构性质对 G' 都成立，且反之亦然，则称它们是*同构的*. 例如，设 G 是形如

$$\begin{bmatrix}1 & x\\ & 1\end{bmatrix}$$

的实矩阵的集合. 它是 $GL_2(\mathbb{R})$的子群，两个矩阵的乘积为

$$\begin{bmatrix}1 & x\\ & 1\end{bmatrix}\begin{bmatrix}1 & y\\ & 1\end{bmatrix} = \begin{bmatrix}1 & x+y\\ & 1\end{bmatrix}.$$

当矩阵相乘时，右上角的元素相加而其余元素不变. 因而当计算这样的矩阵时，只需要考虑右上角的元素. 这一事实正式地表达为 G 与实数加群同构.

如何精确地给出同构的概念并非直接显然的，正确的方法是将其元素用一一对应联系起来，并且与合成法则相容，即一个对应

48

【3.1】
$$G \leftrightarrow G'$$

具有这样的性质：如果 a，$b \in G$ 对应于 a'，$b' \in G'$，则 G 中的积 ab 对应于 G' 中的积 $a'b'$. 这时，群结构的所有性质可由一个群搬到另一个群上.

例如，同构的群 G 和 G' 的单位元互相对应. 为此，设 G 的单位元 1 对应 G' 的元 ε'，而 a'

是G'的任意元素，设a是G中的对应元素．根据假设，积对应到积．因为在G中有$1a=a$，从而在G'中有$\varepsilon'a'=a'$．这样，我们证明了$\varepsilon'=1'$．再例如，对应元素的阶相等．若a对应于G'中的元a'，则由于对应与合成法则相容，$a^r=1$当且仅当$a'^r=1'$．

因为两个同构的群有同样的性质，所以在非正式场合把它们等同起来通常是方便的．例如，$\{1,\cdots,n\}$置换的对称群S_n同构于置换矩阵的群，它是$GL_n(\mathbb{R})$的子群，通常我们不区分这两个群．

我们通常将对应(3.1)不对称地写作函数(或映射)$\varphi:G\longrightarrow G'$．从而，群$G$到$G'$的同构$\varphi$是一个与合成法则相容的一一映射．用$\varphi$的函数记号写出这个相容的意义，我们得到条件

【3.2】 $$对所有\ a,b\in G,\quad \varphi(ab)=\varphi(a)\varphi(b).$$

等式左边表示先在G中让a，b相乘，然后应用φ，而等式右边是前面记为a'，b'的元素$\varphi(a)$和$\varphi(b)$在G'中相乘．这一条件也可以写作

$$(ab)'=a'b'.$$

当然，取作同构定义域的G是任意的，用逆映射$\varphi^{-1}:G'\longrightarrow G$也是可以的．

若存在一个同构$\varphi:G\longrightarrow G'$，则称群$G$与$G'$是同构的．我们有时用符号$\approx$表示两个群同构：

【3.3】 $$G\approx G'\ 表示\ G\ 与\ G'\ 同构.$$

例如，设$C=\{\cdots,a^{-2},a^{-1},1,a,a^2,\cdots\}$为一个无限循环群，则由$\varphi(n)=a^n$定义的映射

$$\varphi:\mathbb{Z}^+\longrightarrow C$$

是一个同构．由于定义域用加法记号而值域用乘法记号，这时条件(3.2)成为$\varphi(m+n)=\varphi(m)\varphi(n)$，或者

$$a^{m+n}=a^m a^n.$$

再举一个简单的例子：设$G=\{1,x,x^2,\cdots,x^{n-1}\}$和$G'=\{1,y,y^2,\cdots,y^{n-1}\}$为两个循环群，由具有相同阶的元素$x$，$y$生成．于是将$x^i$映到$y^i$的映射是同构：同阶的两个循环群同构．

总之，如果存在同构映射$\varphi:G\longrightarrow G'$，即与合成法则相容的一一映射，则两个群$G$与$G'$是同构的．与$G$同构的群组成所谓$G$的同构类，一个同构类中的任意两个群是同构的．当讲到对群分类时，是指要刻画同构类．对所有的群来说，这个问题太难，但作为例子我们后面将会看到，存在一个3阶群的同构类[见(6.13)]、两个4阶群的同构类和五个12阶群的同构类[见第六章(5.1)]．

关于同构，容易引起混乱的是存在群G到其自身的同构：

$$\varphi:G\longrightarrow G.$$

这样的同构称为G的自同构．当然，恒等映射是自同构，但几乎总存在其他的自同构．例如，设$G=\{1,x,x^2\}$为3阶循环群，从而$x^3=1$．交换x和x^2的对换是G的一个自同构：

$$1\rightsquigarrow 1$$
$$x\rightsquigarrow x^2$$
$$x^2\rightsquigarrow x.$$

这是由于x^2是群中的另一个3阶元素．如果把这个元素叫做y，则由于$y^2=x$，因此y生成的循环子群$\{1,y,y^2\}$是整个群G．同构对G作为循环群的这两个实现进行比较．

最重要的自同构的例子是共轭：设$b\in G$是一个给定的元素．关于b的共轭是G到其自身

49

的映射 φ，定义如下：

【3.4】 $$\varphi(x) = bxb^{-1}.$$

它是一个自同构．这是因为，首先，它与群 G 的乘法相容：

$$\varphi(xy) = bxyb^{-1} = bxb^{-1}byb^{-1} = \varphi(x)\varphi(y),$$

其次，由于它有逆函数，即关于 b^{-1} 的共轭，故它是一一映射．如果 G 是阿贝尔群，则共轭是恒等映射：$bab^{-1}=abb^{-1}=a$．但任意非交换群有非平凡的共轭，因此有非平凡的自同构．

元素 bab^{-1} 称为元素 a 关于 b 的共轭，以后会常常遇到．如果 $a'=bab^{-1}$ 对 $b\in G$ 成立，则称 G 中的两个元素 a，a' 是共轭的．共轭元素的行为与元素 a 自身的行为非常相似，例如它在群中的阶是一样的．这可由它是元素 a 在一个自同构下的象这一事实得到．

50

共轭有一个虽然平凡但很有用的解释．即若记 bab^{-1} 为 a'，则

【3.5】 $$ba = a'b.$$

从而我们可以认为关于 b 的共轭是当 b 从一边移到另一边时 a 的变化．

第四节 同 态

设 G，G' 为群．同态是任意映射 $\varphi: G \longrightarrow G'$，满足法则

【4.1】 $$\varphi(ab) = \varphi(a)\varphi(b),$$

对所有 a，$b\in G$．这是与同构相同的要求[见(3.2)]．区别是这里不要求 φ 是双射．

【4.2】例 下列映射是同态：

(a) 行列式函数 $\det: GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$．

(b) 置换的符号 $\mathrm{sign}: S_n \longrightarrow \{\pm 1\}$[见第一章(4.9)]．

(c) 映射 $\varphi: \mathbb{Z}^+ \longrightarrow G$，由 $\varphi(n)=a^n$ 定义，其中 a 是 G 中给定的元素．

(d) 子群 H 到群 G 的包含映射 $i: H \longrightarrow G$，由 $i(x)=x$ 定义．

【4.3】命题 *群同态 $\varphi: G \longrightarrow G'$ 将单位元对应到单位元，将逆元对应到逆元．换言之，$\varphi(1_G)=1_{G'}$ 且 $\varphi(a^{-1})=\varphi(a)^{-1}$．*

证明 因为 $1=1\cdot 1$ 及 φ 为同态，所以 $\varphi(1)=\varphi(1\cdot 1)=\varphi(1)\varphi(1)$．由(1.12)在两边消去 $\varphi(1)$ 得 $1=\varphi(1)$．接下来，$\varphi(a^{-1})\varphi(a)=\varphi(a^{-1}a)=\varphi(1)=1$，类似地有 $\varphi(a)\varphi(a^{-1})=1$．于是 $\varphi(a^{-1})=\varphi(a)^{-1}$． ■

每一个群同态 φ 确定两个重要的子群：它的象和它的核．同态 $\varphi: G \longrightarrow G'$ 的象很容易理解．它是映射的象

【4.4】 $$\mathrm{im}\varphi = \{x \in G' \mid \text{对某个 } a \in G, \text{有 } x = \varphi(a)\},$$

并且它是 G' 的一个子群．象的另一个记号是 $\varphi(G)$．在例(4.2a、b)中，象等于映射的值域，但在(4.2c)中，它是 a 生成的 G 的循环子群，而在(4.2d)中它是子群 H．

φ 的核较为费解．它是被映为 G' 中单位元的 G 中的元素的集合：

51

【4.5】 $$\ker\varphi = \{a \in G \mid \varphi(a) = 1\},$$

也可以将它刻画为单位元的原象 $\varphi^{-1}(1)$[见附录(1.5)]．核是 G 的子群，因为若 a 和 b 在 $\ker\varphi$ 中，则 $\varphi(ab)=\varphi(a)\varphi(b)=1\cdot 1=1$，于是 $ab\in\ker\varphi$，等等．

行列式同态的核是由行列式为 1 的矩阵构成的群. 这个子群称为特殊线性群, 记为 $SL_n(\mathbb{R})$:

【4.6】 $$SL_n(\mathbb{R}) = \{n \times n \text{ 实矩阵 } A \mid \det A = 1\},$$

它是 $GL_n(\mathbb{R})$的一个子群. 前面例(4.2b)中符号同态的核称为交错群, 记为 A_n:

【4.7】 $$A_n = \{\text{偶置换}\},$$

它是 S_n 的一个子群. (4.2d)中同态的核是使 $a^n=1$ 的整数 n 的集合. 前面在(2.8)中证明了这是$\mathbb{Z}^+$ 的一个子群.

除了是一个子群外, 同态的核还有另外一个虽然不易理解但却十分重要的性质. 即若 a 在 $\ker\varphi$ 中而 b 是群 G 的任意元素, 则其共轭 bab^{-1}亦在 $\ker\varphi$ 中. 因为 $a\in\ker\varphi$ 意味着 $\varphi(a)=1$. 从而

$$\varphi(bab^{-1}) = \varphi(b)\varphi(a)\varphi(b^{-1}) = \varphi(b)1\varphi(b)^{-1} = 1,$$

于是也有 $bab^{-1}\in\ker\varphi$.

【4.8】定义 群 G 的一个子群 N 称为**正规子群**, 如果它具有下列性质: 对每一个 $a\in N$ 和每一个 $b\in G$, 共轭 bab^{-1}属于 N.

如我们上面所看到的,

【4.9】 同态的核是正规子群.

这样 $SL_n(\mathbb{R})$是 $GL_n(\mathbb{R})$的一个正规子群, 而 A_n 是 S_n 的一个正规子群.

一个阿贝尔群 G 的任意子群皆是正规的, 因为当 G 是阿贝尔群时, 总有 $bab^{-1}=a$. 但非阿贝尔群的子群不一定是正规的. 例如, 可逆上三角矩阵的群 T 不是 $GL_2(\mathbb{R})$的正规子群. 这是因为, 如果令$A=\begin{bmatrix}1 & 1\\ & 1\end{bmatrix}$而 $B=\begin{bmatrix} & 1\\ 1 & \end{bmatrix}$, 则 $BAB^{-1}=\begin{bmatrix}1 & \\ 1 & 1\end{bmatrix}$. 这时 $A\in T$ 而 $B\in GL_n(\mathbb{R})$, 但 $BAB^{-1}\notin T$.

群 G 的中心, 有时记为 Z 或 $Z(G)$, 是 G 中与每个元素交换的元素的集合:

【4.10】 $$Z = \{z \in G \mid \text{对所有 } x \in G, \text{有 } zx = xz\}.$$

任意群的中心是这个群的一个正规子群. 例如, 可以证明 $GL_n(\mathbb{R})$的中心为标量矩阵, 即形如 cI 的矩阵.

52

第五节 等价关系和划分

一个基本的数学构造是从一个集合 S 出发, 根据给定的法则等同 S 的元素而得到新的集合. 例如, 可以将整数分成两类, 即偶数和奇数. 或者, 可以将平面上的全等三角形视为等价的几何对象. 这个非常一般的过程来自不同的方面, 我们现在就讨论这些方面.

设 S 为集合. S 的一个划分 P 是将 S 分为互不重叠的子集:

【5.1】 $$S = \text{不交、非空子集的并}.$$

例如, 集合

$$\{1,3\},\{2,5\},\{4\}$$

是集合$\{1, 2, 3, 4, 5\}$的一个划分. 奇数集合和偶数集合这两个集合构成所有整数集合$\mathbb{Z}$的一个划分.

S 上的等价关系是 S 中某些元素的关系. 我们通常将它记为 $a\sim b$, 并称为 a 与 b 的一个等价.

【5.2】一个等价关系要求是

(i) 传递的: 若 $a\sim b$ 且 $b\sim c$, 则 $a\sim c$.

(ii) 对称的：若 $a \sim b$，则 $b \sim a$.

(iii) 自反的：对所有 $a \in S$ 有 $a \sim a$.

三角形的全等是平面上三角形的集合 S 上的等价关系的例子.

从形式上讲，S 上的一个关系与元素对的集合 $S \times S$ 的一个子集 R 是同一个东西，也就是说子集 R 由满足 $a \sim b$ 的元素对 (a, b) 构成. 用这个子集的语言，我们可将等价关系的公理写成如下形式：(i)若 $(a, b) \in R$ 且 $(b, c) \in R$，则 $(a, c) \in R$；(ii)若 $(a, b) \in R$，则 $(b, a) \in R$；(iii)对所有 a 有 $(a, a) \in R$.

集合 S 的划分和 S 上的等价关系这两个概念在逻辑上是等价的，虽然实际上给出的通常只是二者之一. 给定 S 上的划分 P，可用下面的规则定义一个等价关系 R：如果 a 和 b 属于划分的同一个集合，则 $a \sim b$. 公理(5.2)显然成立. 反之，给定等价关系 R，可以这样定义划分 P：含 a 的子集是所有满足条件 $a \sim b$ 的元素 b 的集合. 这个子集称为 a 的等价类，于是 S 被划分为等价类.

我们来看一看划分一个集合 S 的等价类. 用 C_a 记一个元素 $a \in S$ 的等价类. 则 C_a 由满足 $a \sim b$ 的元素 b 组成：

53

【5.3】
$$C_a = \{b \in S \mid a \sim b\}.$$

自反公理告诉我们 $a \in C_a$. 因此类 C_a 非空，并且由于 a 可以是任意元素，故这些类覆盖 S. 还剩下需要证明的划分的性质是等价类间没有重叠部分. 这里容易糊涂，因为如果 $a \sim b$ 则由定义 $b \in C_a$. 但同时还有 $b \in C_b$. 这是否表明 C_a 与 C_b 重叠呢？我们要记住符号 C_a 是用来表示以某种方式定义的 S 的子集的记号. 划分由子集而不是记号构成. 的确 C_a 和 C_b 有 b 作为其公共元素，但那没有问题，因为它们是同一个集合的两个不同的记号. 我们将证明下面的结论：

【5.4】 *设 C_a 与 C_b 有一个公共元素 d，则 $C_a = C_b$.*

我们首先指出若 $a \sim b$，则 $C_a = C_b$. 为此，设 x 是 C_b 的一个任意元素，则 $b \sim x$. 因为 $a \sim b$，传递性指出 $a \sim x$，于是 $x \in C_a$. 因此 $C_b \subset C_a$. 相反的包含通过交换 a 和 b 的角色得到. 要证(5.4)，设 d 属于 C_a 也属于 C_b，则 $a \sim d$ 且 $b \sim d$. 由前面所指出的，$C_a = C_d = C_b$，这正是要证的. ■

设在 S 上给定一个等价关系或划分. 则我们可以构造一个新的集合 $\overline{S}$，其元素是等价类或组成划分的子集. 为了简化记号，常把 a 所在的等价类或划分中包含 a 的子集记为 $\overline{a}$. 这样 $\overline{a}$ 是 $\overline{S}$ 的元素.

注意存在一个自然的满射

【5.5】
$$S \longrightarrow \overline{S},$$
$$a \rightsquigarrow \overline{a}.$$

在 $S = \mathbb{Z}$ 的划分的最初例子中，$\overline{S}$ 中含有两个元素——(偶)和(奇)，其中(偶)表示偶数集合而(奇)表示奇数集合. 并且有 $\overline{0} = \overline{2} = \overline{4}$，等等. 因而可以用这些记号中的任一个表示集合(偶). 映射

【5.6】
$$\mathbb{Z} \longrightarrow \{(偶),(奇)\}$$

是显而易见的.

理解这一构造的方式有两种. 我们可以想象把 S 中的元素放到分开的堆里，划分里的每个子集放一堆，然后把堆看成新集合 $\overline{S}$ 的元素. 映射 $S \longrightarrow \overline{S}$ 将每一元素与它的堆对应. 或者，

也可以考虑改变我们关于 S 中元素相等的意义，将 $a\sim b$ 解释为在 $\overline{S}$ 中 $a=b$. 用这种方式去看，两个集合 S 与 $\overline{S}$ 中的元素对应，而在 $\overline{S}$ 中有更多的元素相互相等. 这正是我们在中学中处理全等三角形的方式. (5.5)中上面划横的符号很适合这种直观图像. 我们可以用与 S 中同样的符号，但在其上面加一横提醒我们新的规则：

【5.7】
$$\overline{a}=\overline{b} \text{ 意为 } a\sim b.$$
这个记号通常是非常方便的.

54

上面划横的符号的缺点是许多符号所表示的都是 $\overline{S}$ 中的同一个元素. 有时这一缺点可以通过在每一等价类中自始至终选择一个特殊元素，也就是它的代表的办法来克服. 例如，习惯上用 $\overline{0}$ 代表(偶)而用 $\overline{1}$ 代表(奇)：

【5.8】
$$\{(\text{偶}),(\text{奇})\}=\{\overline{0},\overline{1}\}.$$

虽然堆的图像较为直接，但是关于 $\overline{S}$ 的第二种方式经常要更好一些，因为堆的运算难于看得出来，而上面划横的符号非常适合于代数的运算.

集合之间的任意映射 $\varphi:S\longrightarrow T$ 在其定义域 S 上定义一个等价关系，也就是由规则"如果 $\varphi(a)=\varphi(b)$ 则 $a\sim b$"给出的等价关系. 我们将称之为**由映射确定的等价关系**. 相应的划分是由 T 中元素的非空逆象组成的. 由定义，一个元素 $t\in T$ 的**逆象**是由所有满足条件 $\varphi(s)=t$ 的元素 s 组成的 S 的子集. 用符号表示为

【5.9】
$$\varphi^{-1}(t)=\{s\in S\mid \varphi(s)=t\}.$$
这样 $\varphi^{-1}(t)$ 是定义域 S 的子集，由元素 $t\in T$ 确定. (这只是一个记号，要记住的是 φ^{-1} 通常不是一个函数.)逆象也可以叫做映射 φ 的**纤维**. 纤维 $\varphi^{-1}(t)$ 非空表明 t 属于 φ 的象，这些纤维构成 S 的一个划分. 这里等价类的集合 $\overline{S}$，也就是非空纤维的集合，还有另一个含义，即作为映射的象 $\mathrm{im}\varphi$. 也就是说有一个一一映射

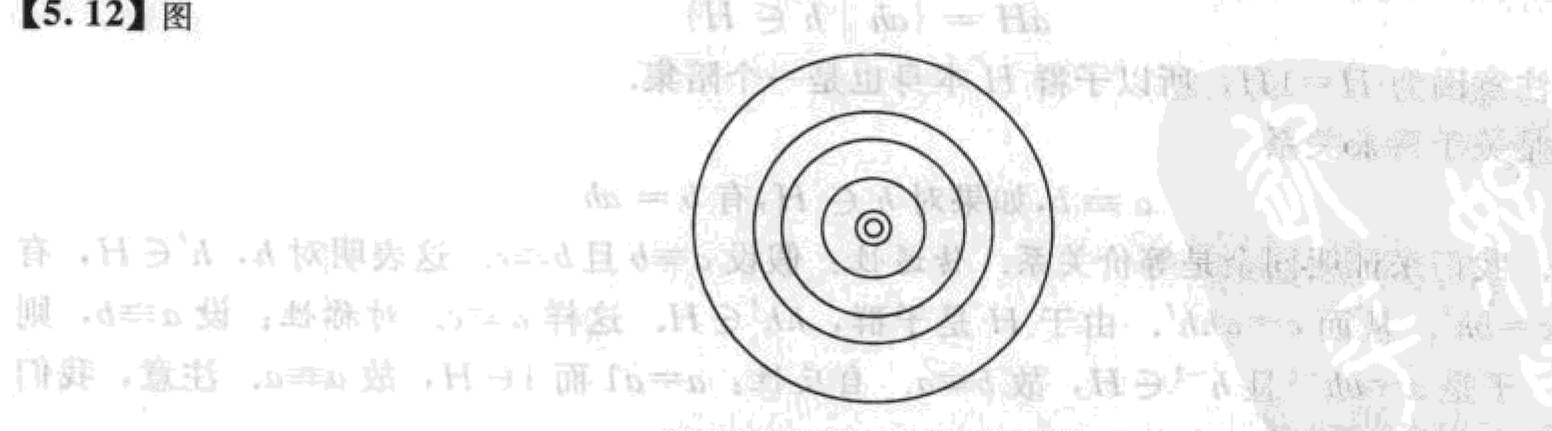
【5.10】
$$\overline{\varphi}:\overline{S}\longrightarrow \mathrm{im}\varphi,$$
将 $\overline{S}$ 的元 $\overline{s}$ 映到 $\varphi(s)$.

现在我们回到群同态. 设 $\varphi:G\longrightarrow G'$ 为一同态，我们来分析与映射 φ 对应的 G 上的等价关系，或等价地，同态的纤维. 这个关系通常用$\equiv$而不是$\sim$表示，并称之为**同余**：

【5.11】
$$a\equiv b,\text{如果 } \varphi(a)=\varphi(b).$$

例如，设 $\varphi:\mathbb{C}^{\times}\longrightarrow\mathbb{R}^{\times}$ 是由 $\varphi(a)=|a|$ 定义的绝对值同态. 诱导的等价关系是 $a\equiv b$，如果 $|a|=|b|$. 这一映射的纤维是圆心为 0 的同心圆. 它们与 $\mathrm{im}\varphi$ 的元素，即正实数集有一一映射.

【5.12】 图



绝对值映射 $\mathbb{C}^{\times}\longrightarrow\mathbb{R}^{\times}$ 的纤维

55

关系(5.11)可以用多种方式重新写出，对我们来说下面这一个最重要：

【5.13】命题 设 $\varphi:G\longrightarrow G'$ 是核为 N 的群同态，a，b 为 G 的元素. 则 $\varphi(a)=\varphi(b)$ 当且仅当对某个元素 $n\in N$ 有 $b=an$，或等价地，$a^{-1}b\in N$.

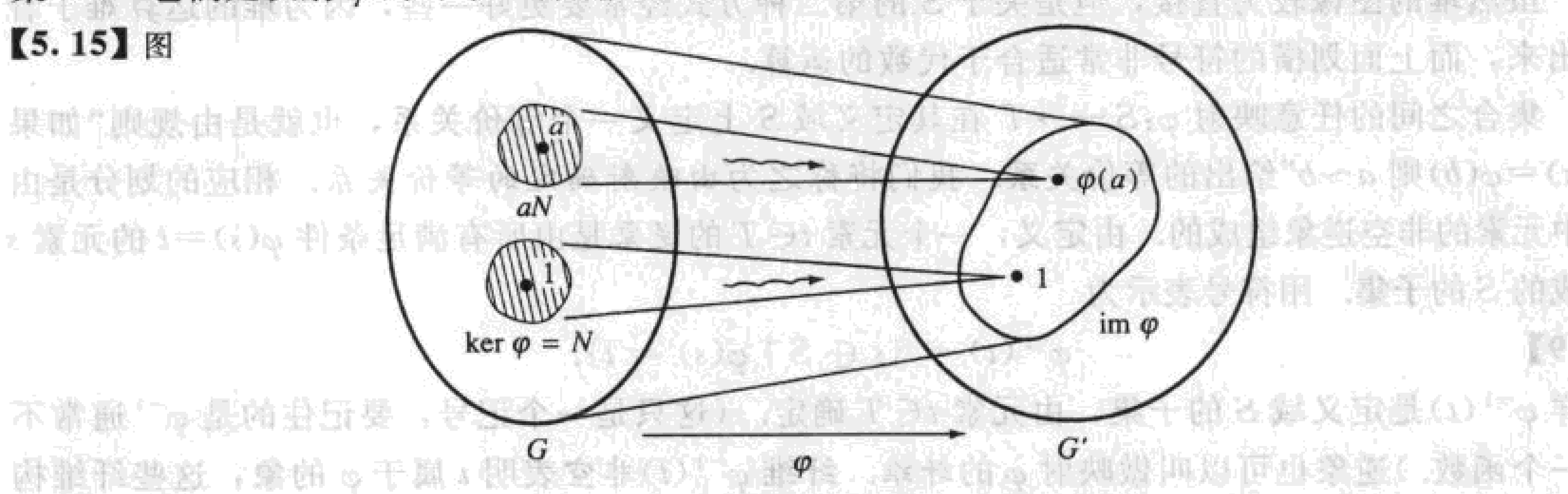
证明 设 $\varphi(a)=\varphi(b)$. 则 $\varphi(a)^{-1}\varphi(b)=1$，由于 φ 为同态，我们可以用(4.1)和(4.3)将这个等式重新写为 $\varphi(a^{-1}b)=1$. 由定义，核 N 是所有满足 $\varphi(x)=1$ 的元素 $x\in G$ 的集合. 这样 $a^{-1}b\in N$，或者说对某 $n\in N$ 有 $a^{-1}b=n$. 于是 $b=an$，这正是要证明的. 反过来，如果对 $n\in N$ 有 $b=an$，则 $\varphi(b)=\varphi(a)\varphi(n)=\varphi(a)1=\varphi(a)$. ■

形如 an 的元素的集合记作 aN，称为 N 在 G 中的陪集：

【5.14】
$$aN=\{g\in G\mid g=an,\text{对某 } n\in N\}.$$

因而，陪集 aN 是与 a 同余的所有群的元素 b 的集合. 同余关系 $a\equiv b$ 将群 G 划分为同余类，即陪集 aN. 它们是映射 φ 的纤维. 特别是，(5.12)中所示的关于中心的圆是绝对值同态的陪集.

【5.15】图



群同态的示意图

一个值得注意的重要情形是核为平凡子群. 在这一情形，(5.13)表述如下：

【5.16】推论 群同态 $\varphi:G\longrightarrow G'$ 是单射当且仅当其核为平凡子群 $\{1\}$.

这给出了证明一个同态是同构的方法. 为此，我们验证 $\ker\varphi=\{1\}$，从而 φ 为单射，且还有 $\operatorname{im}\varphi=G'$，即 φ 也是满射.

56

第六节 陪 集

无论是对同态核，还是对群 G 的任意子群 H，都可以定义陪集. *左陪集*是一个具有形式

【6.1】
$$aH=\{ah\mid h\in H\}$$

的子集. 注意因为 $H=1H$，所以子群 H 本身也是一个陪集.

陪集是关于同余关系

【6.2】
$$a\equiv b,\text{如果对 } h\in H,\text{有 } b=ah$$

的等价类. 我们来证明同余是等价关系. *传递性*：假设 $a\equiv b$ 且 $b\equiv c$. 这表明对 h，$h'\in H$，有 $b=ah$ 和 $c=bh'$. 从而 $c=ahh'$. 由于 H 是子群，$hh'\in H$. 这样 $a\equiv c$. *对称性*：设 $a\equiv b$，则有 $b=ah$. 于是 $a=bh^{-1}$ 且 $h^{-1}\in H$，故 $b\equiv a$. *自反性*：$a=a1$ 而 $1\in H$，故 $a\equiv a$. 注意，我们用到子群定义的所有性质.

因为等价类构成划分，我们得到下面的推论：

【6.3】**推论** 子群的左陪集是群的划分.

【6.4】**注** 记号 aH 定义 G 的某个子集. 与任意等价关系一样，不同的记号可以表示同一个集合. 事实上，我们知道 aH 是包含 a 的唯一陪集，因而

【6.5】 $aH = bH$ 当且仅当 $a \equiv b$.

推论只是(5.4)的复述：

【6.6】如果 aH 和 bH 有一个公共元素，则它们相等.

例如，设 G 是对称群 S_3，以(1.18)给出的方式表出：$G=\{1, x, x^2, y, xy, x^2y\}$. 元素 xy 的阶为 2，因而它生成一个 2 阶循环子群 $H=\{1, xy\}$. H 在 G 中的左陪集是三个子集

【6.7】 $\{1,xy\} = H = xyH$, $\{x,x^2y\} = xH = x^2yH$, $\{x^2,y\} = x^2H = yH$.

注意，它们的确划分了群.

一个子群的左陪集数称为 H 在 G 中的**指标**，并记为

【6.8】 $$[G:H].$$

这样，在我们的例子中指标是 3. 当然，如果群中含有无限多个元素，指标可以是无限的.

57

注意，存在一个由子群 H 到陪集 aH 的双射，使 $h \rightsquigarrow ah$. (为什么这个映射是双射呢?)这样

【6.9】陪集 aH 的元素个数与 H 的元素个数一样多.

因为 G 是 H 的陪集并且这些陪集互不重叠，我们得到了重要的计数公式：

【6.10】 $$|G| = |H|[G:H],$$

如同(2.10)一样，其中 $|G|$ 表示 G 的阶，如果某项为无穷，等式的意义是显然的. 在例(6.7)中，这个公式成为 $6=2 \cdot 3$.

方程(6.10)右边两项一定整除左边这一事实是非常重要的. 下面是这些结果中的一个，正式的叙述是：

【6.11】**推论** 拉格朗日定理：设 G 是有限群且 H 是 G 的子群. H 的阶整除 G 的阶.

第二节我们定义一个元素 $a \in G$ 的阶为 a 生成的循环子群的阶. 因而由拉格朗日定理得到下面的结论：

【6.12】元素的阶整除群的阶.

这个事实有一个值得注意的结果.

【6.13】**推论** 设群 G 有 p 个元素且 p 是素整数. 设 $a \in G$ 是任意元，不是单位元. 则 G 是由 a 生成的循环群 $\{1, a, \cdots, a^{p-1}\}$.

因为 $a \neq 0$，a 的阶大于 1 且它整除 $|G| = p$. 因此它等于 p. 因为 G 的阶为 p，所以 $\{1, a, \cdots, a^{p-1}\}$ 就是整个群.

这样我们就对所有素数阶 p 的群作了分类. 它们构成一个同构类，即 p 阶循环群类.

计数公式也可应用于一个给定的同态. 设 $\varphi: G \longrightarrow G'$ 是一个同态. 正如我们在(5.13)所看到的，$\ker\varphi$ 的左陪集是映射 φ 的纤维. 它们与象中的元素一一对应.

【6.14】 $$[G:\ker\varphi] = |\mathrm{im}\varphi|.$$

这样由(6.10)得到下面的推论：

【6.15】**推论** 设 $\varphi: G \longrightarrow G'$ 是有限群的一个同态. 则

$$|G| = |\ker\varphi| \cdot |\mathrm{im}\varphi|.$$

这样 $|\ker\varphi|$ 整除 $|G|$，而 $|\mathrm{im}\varphi|$ 同时整除 $|G|$ 和 $|G'|$.

证明 公式由(6.10)和(6.14)合起来得到，而且它推出 $|\ker\varphi|$ 和 $|\mathrm{im}\varphi|$ 整除 $|G|$. 因为 $\mathrm{im}\varphi$ 是 G' 的子群，所以 $|\mathrm{im}\varphi|$ 也整除 $|G'|$. ■

58

我们暂时回到陪集的定义. 这里使用的是左陪集 aH. 也可以定义子群 H 的右陪集并且重复上面的讨论. 子群 H 的右陪集是集合

【6.16】 $$Ha = \{ha \mid h \in H\},$$

它们是等价关系(右同余)

$$a \equiv b, \text{如果存在 } h \in H \text{ 使 } b = ha$$

的等价类. 右陪集和左陪集不一定相同. 例如，S_3 的子群 $\{1, xy\}$ 的右陪集是

【6.17】 $\{1, xy\} = H = Hxy$，$\{x, y\} = Hx = Hy$，$\{x^2, x^2y\} = Hx^2 = Hx^2y$.

S_3 的这个划分不同于左陪集的划分(6.7).

然而，若 N 是正规子群，则左、右陪集相同.

【6.18】命题 群 G 的子群 H 是正规的当且仅当每一个左陪集也是右陪集. 若 H 是正规的，则对每个 $a \in G$，有 $aH = Ha$.

证明 设 H 是正规的. 对任意 $h \in H$ 和任意 $a \in G$，有

$$ah = (aha^{-1})a.$$

因为 H 是正规子群，所以共轭元素 $k = aha^{-1}$ 属于 H. 这样元素 $ah = ka$ 属于 aH 也属于 Ha. 这证明了 $aH \subset Ha$. 类似地有 $Ha \subset aH$，因而这两个陪集相等. 反过来，设 H 不是正规的，则存在元素 $h \in H$ 和 $a \in G$ 使得 aha^{-1} 不属于 H. 这样 ah 属于左陪集 aH 但不属于右陪集 Ha. 如果它属于右陪集 Ha，设 $ah = h'a$ 对某个 $h' \in H$ 成立，则我们会有 $aha^{-1} = h' \in H$，这与假设矛盾. 另一方面，aH 与 Ha 有一个公共元素，即元素 a. 于是 aH 不会是其他的右陪集. 这证明划分成左陪集与划分成右陪集是不相同的. ■

第七节 限制到子群的同态

要理解一个复杂的群，通常的方法是研究某些不太复杂的子群. 如果有可能在群论中选出一个最重要的方法的话，那就应该是这个. 例如，一般线性群 GL_2 比可逆上三角矩阵组成的群复杂. 我们希望回答关于上三角矩阵的任何问题. 用上、下三角矩阵做乘积，可以涵盖群 GL_2 的绝大部分. 当然，其诀窍是从对子群的理解得到关于群本身的信息. 这应该怎么做，我们并没有一个一般的法则. 但只要对群进行新的构造，就应当研究它对于子群的影响. 这就是限制到子群的意思. 本节我们将对子群和同态这样处理.

59

设 H 是 G 的子群. 我们先考虑还有另一个给定子群 K 的情形. K 限制到 H 正是交 $K \cap H$. 下面的命题是个简单的练习.

【7.1】命题 两个子群的交 $K \cap H$ 是 H 的一个子群. 如果 K 是 G 的正规子群，则 $K \cap H$ 是 H 的正规子群.

这里没有太多可说的，但如果 G 是有限群，我们可以应用计数公式(6.10)，特别是应用拉

格朗日定理得到关于交的信息．也就是说，$K\cap H$ 是 H 的一个子群也是 K 的一个子群．从而，其阶同时整除阶 $|H|$ 和 $|K|$．如果 $|H|$ 和 $|K|$ 没有公因子，则可以得到 $K\cap H=\{1\}$．

假设给定同态 $\varphi:G\longrightarrow G'$，而且和上面一样，$H$ 是 G 的一个子群．则可以限制 φ 到 H 得到一个同态

【7.2】 $$\varphi|_H:H\longrightarrow G'.$$

这是指取相同的映射 φ 但将其定义域限制到 H．换言之，对所有 $h\in H$ 有 $\varphi|_H(h)=\varphi(h)$．因为 φ 是同态，所以它的限制也是．

$\varphi|_H$的核是 $\ker\varphi$ 与 H 的交

【7.3】 $$\ker\varphi|_H=(\ker\varphi)\cap H.$$

由核的定义这是很明显的：$\varphi(h)=1$ 当且仅当 $h\in\ker\varphi$．

计数公式也可以帮助描述这个限制．因为 $\varphi|_H$的象是 $\varphi(H)$．根据推论(6.15)，$|\varphi(H)|$ 同时整除 $|H|$ 和 $|G'|$．因而，如果 $|H|$ 和 $|G'|$ 没有公因子，则 $\varphi(H)=\{1\}$．则我们可得 $H\subset\ker\varphi$．

例如，置换的符号用同态(4.2b)——$S_n\longrightarrow\{\pm1\}$描述．同态的值域的阶为 2，其核是交错群．如果 S_n 的子群 H 为奇数阶，则同态限制到子群 H 为平凡的，这表明 H 包含在交错群中，也就是说，H 由偶置换构成．当 H 是由一个在群中阶为奇数的置换 p 生成的循环子群时，就是这样的．由此得到每一个奇数阶的置换为偶置换．另一方面，我们不能对偶数阶的置换得出任何结论．它们可以是奇的，也可以是偶的．

当给出一个同态 $\varphi:G\longrightarrow G'$ 和 G' 的一个子群 H' 时，我们也可以把同态 φ 限制到 H' 上．这里，要把 φ 的定义域适当地缩小，以得到一个映到 H' 的映射．自然的做法是尽可能缩小定义域，也就是取 H' 的整个逆象．

【7.4】命题 设 $\varphi:G\longrightarrow G'$是一个同态，并且设 H'是 G'的子群．用$\widetilde{H}$记逆象 $\varphi^{-1}(H')=\{x\in G\mid\varphi(x)\in H'\}$．则

(a) $\widetilde{H}$是 G 的子群．

(b) 如果 H'是 G'的正规子群，则$\widetilde{H}$是 G 的正规子群．

(c) $\widetilde{H}$包含 $\ker\varphi$．

(d) φ 限制到$\widetilde{H}$定义一个同态$\widetilde{H}\longrightarrow H'$，其核为 $\ker\varphi$．

例如，考虑行列式同态 $\det:GL_n(\mathbb{R})\longrightarrow\mathbb{R}^{\times}$．则正实数集合 P 是$\mathbb{R}^{\times}$的子群，且其逆象是具有正行列式的 $n\times n$ 可逆矩阵的集合，这是 $GL_n(\mathbb{R})$的正规子群．

60

命题(7.4)的证明 这个证明也是简单的练习，但要记住 φ^{-1}不是一个映射．由定义，$\widetilde{H}$是使 $\varphi(x)\in H'$的元素 $x\in G$ 的集合．我们验证子群的条件．单位元：因为 $\varphi(1)=1\in H'$，所以 $1\in\widetilde{H}$．封闭性：设 x，$y\in\widetilde{H}$．这意味着 $\varphi(x)$和 $\varphi(y)$都属于 H'．因为 H'是子群，所以 $\varphi(x)\varphi(y)\in H'$．由于 φ 是同态，$\varphi(x)\varphi(y)=\varphi(xy)\in H'$．因此 $xy\in\widetilde{H}$．逆元：设 $x\in\widetilde{H}$，则有 $\varphi(x)\in H'$；于是因为 H'是子群，$\varphi(x)^{-1}\in H'$．由于 φ 是同态，$\varphi(x)^{-1}=\varphi(x^{-1})$．这样 $x^{-1}\in\widetilde{H}$．

设 H'是一个正规子群，且设 $x\in\widetilde{H}$和 $g\in G$．则 $\varphi(gxg^{-1})=\varphi(g)\varphi(x)\varphi(g)^{-1}$，且 $\varphi(x)\in$

H'. 于是 $\varphi(gxg^{-1})\in H'$，这就证明了 $gxg^{-1}\in\widetilde{H}$. 接下来，$\widetilde{H}$包含 $\ker\varphi$，这是因为，若 $x\in\ker\varphi$，则 $\varphi(x)=1$，而 $1\in H'$. 故 $x\in\varphi^{-1}(H')$. 最后一个断言应该是显而易见的. ■

第八节 群 的 积

设 G，G'为两个群. 积集 $G\times G'$可按分量乘积构成一个群. 即对 a，$b\in G$ 和 a'，$b'\in G'$，我们用规则

【8.1】
$$(a,a')(b,b')\rightsquigarrow(ab,a'b')$$

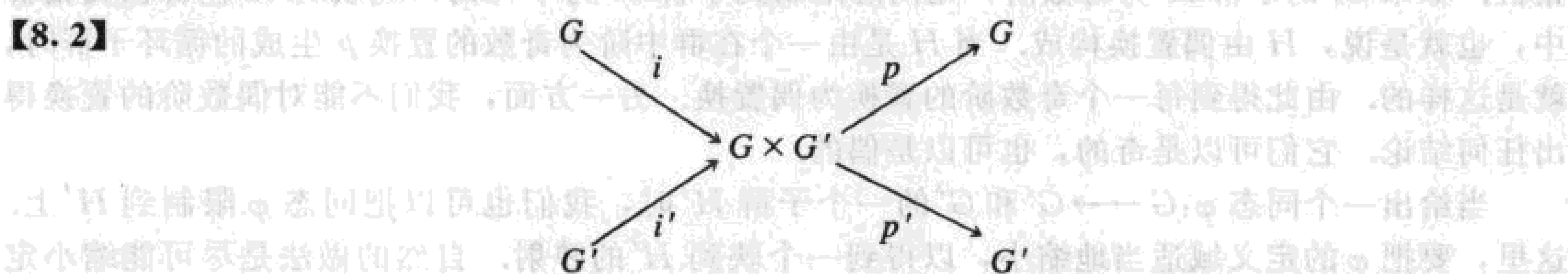
定义元素对的乘积. 元素对(1，1)是单位元，而$(a,a')^{-1}=(a^{-1},a'^{-1})$. $G\times G'$上的结合律由 G 和 G'上的结合律得到. 这样得到的群称为 G 与 G'的积，记作 $G\times G'$. 其阶是 G 与 G'的阶的乘积.

积群以简单的方式与其因子 G 和 G'相联系，我们可用由

$$i(x)=(x,1),\quad i'(x')=(1,x'),$$
$$p(x,x')=x,\quad p'(x,x')=x'$$

定义的同态的语言加以总结.

【8.2】



61

映射 i，i'是单射，可用来将 G，G'等同于 $G\times G'$的子群 $G\times1$，$1\times G'$. 映射 p，p'是满射，$\ker p=1\times G'$而 $\ker p'=G\times1$. 这两个映射称为投影. 作为核，$G\times1$ 和 $1\times G'$是 $G\times G'$的正规子群.

【8.3】命题 积的映射性质：设 H 是任意群. 同态 $\Phi:H\longrightarrow G\times G'$与同态对$(\varphi,\varphi')$间一一对应：

$$\varphi:H\longrightarrow G,\quad \varphi':H\longrightarrow G'.$$

Φ 的核是交$(\ker\varphi)\cap(\ker\varphi')$.

证明 给定一对同态(φ,φ')，通过规则 $\Phi(h)=(\varphi(h),\varphi'(h))$定义相应的同态

$$\Phi:H\longrightarrow G\times G'.$$

容易看出这是一个同态. 反之，给定 Φ，通过与投射合成得到 φ 和 φ'如下：

$$\varphi=p\Phi,\quad \varphi'=p'\Phi.$$

显然，$\Phi(h)=(1,1)$当且仅当 $\varphi(h)=1$ 且 $\varphi'(h)=1$，这就证明了 $\ker\Phi=(\ker\varphi)\cap(\ker\varphi')$. ■

显然，大家都期望把一个给定的群 G 分解成积，也就是说找到两个群 H 和 H'，使 G 同构于它们的积 $H\times H'$. 群 H 和 H'都较小因而较简单，而且 $H\times H'$与其因子的关系也容易理解. 可是，给定的群是积的情形非常稀少，但的确偶有发生.

例如，令人惊叹的是 6 阶循环群可以被分解：一个 6 阶循环群 C_6 同构于 2 阶和 3 阶的循环群的积 $C_2\times C_3$. 这可用刚讨论过的映射性质来证明. 设 $C_6=\{1,x,x^2,x^3,x^4,x^5\}$，$C_2=\{1,y\}$，$C_3=\{1,z,z^2\}$. 由 $\varphi(x^i)=(y^i,z^i)$定义的规则

$$\varphi: C_6 \longrightarrow C_2 \times C_3$$

是一个同态，且它的核是使 $y^i=1$ 和 $z^i=1$ 的元素 x^i 的集合. 现有 $y^i=1$ 当且仅当 i 能被 2 整除，而 $z^i=1$ 当且仅当 i 能被 3 整除. 在 1 到 5 之前没有同时能被 2 和 3 整除的整数. 因而 $\ker\varphi=\{1\}$，且 φ 是单射. 因为两个群的阶都是 6，所以 φ 是一一映射，因而是同构.

62

只要两个整数 r 和 s 没有公因子，同样的论证就可用于 rs 阶循环群.

【8.4】命题 设 r，s 是没有公因子的整数. 一个 rs 阶的循环群同构于一个 r 阶循环群和一个 s 阶循环群的积.

另一方面，一个 4 阶循环群不同构于两个 2 阶循环群的积. 因为容易看出，$C_2\times C_2$ 的每个元素的阶为 1 或 2，而 4 阶循环群中含有两个阶为 4 的元素. 还有，命题没有对非循环群给出任何结论.

设 A 和 B 是群 G 的两个子集. 我们记 A 与 B 的元素的积的集合为

【8.5】 $$AB=\{x\in G \mid \text{存在 } a\in A, b\in B \text{ 使得 } x=ab\}.$$

下面的命题刻画了积群.

【8.6】命题 设 H 和 K 是一个群 G 的子群.

(a) 若 $H\cap K=\{1\}$，则由 $p(h,k)=hk$ 定义的积映射 $p: H\times K\longrightarrow G$ 是单的. 其象是子集 HK.

(b) 若 H 或 K 是 G 的正规子群，则积集 HK 与 KH 相等，且 HK 是 G 的子群.

(c) 若 H 和 K 都是正规的，$H\cap K=\{1\}$ 且 $HK=G$，则 G 同构于积群 $H\times K$.

证明 (a) 设 (h_1, k_1)，(h_2, k_2) 为 $H\times K$ 的元，使得 $h_1k_1=h_2k_2$. 在此等式两边左乘 h_1^{-1}，右乘 k_2^{-1}，我们得到 $k_1k_2^{-1}=h_1^{-1}h_2$. 由于 $H\cap K=\{1\}$，$k_1k_2^{-1}=h_1^{-1}h_2=1$，于是 $h_1=h_2$ 且 $k_1=k_2$. 这就证明了 p 是单的.

(b) 设 H 是 G 的正规子群，且设 $h\in H$ 和 $k\in K$. 注意到 $kh=(khk^{-1})k$. 因为是 H 正规的，$khk^{-1}\in H$. 从而 $kh\in HK$，这证明 $KH\subset HK$. 另一个包含的证明是类似的. 现在容易得到 HK 是子群这一事实. 要证对乘法封闭，注意积 $(hk)(h'k')=h(kh')k'$，中间项 kh' 属于 $KH=HK$，比如说 $kh'=h''k''$. 于是 $hkh'k'=(hh'')(k''k')\in HK$. 对取逆封闭的证明是类似的：$(hk)^{-1}=k^{-1}h^{-1}\in KH=HK$. 当然 $1=1\cdot 1\in HK$. 这样 HK 是一个子群. K 正规情形的证明是类似的.

(c) 设两个子群皆正规且 $H\cap K=\{1\}$. 考虑积 $(hkh^{-1})k^{-1}=h(kh^{-1}k^{-1})$. 因为 K 是正规子群，左边属于 K. 因为 H 是正规的，右边属于 H. 因而这个积属于交 $H\cap K$，也就是说 $hkh^{-1}k^{-1}=1$. 因而 $hk=kh$. 知道了这一点，直接得到 p 是同态这一事实：在群 $H\times K$ 中，乘法法则为 $(h_1, k_1)(h_2, k_2)=(h_1h_2, k_1k_2)$，这个元素对应于 G 中的元素 $h_1h_2k_1k_2$，而在 G 中，h_1k_1 和 h_2k_2 的乘积为 $h_1k_1h_2k_2$. 因为 $h_2k_1=k_1h_2$，所以两个积是相等的. 在(a)中证明了 p 为单射，而假设 $HK=G$ 表明 p 是一个满射. ■

63

重要的是要注意，除非两个子群相互可交换，否则乘积映射 $p: H\times K\longrightarrow G$ 将不是一个群同态.

第九节 模 算 术

本节我们讨论高斯的整数同余的定义，这是数论中最重要的概念之一. 本节将针对任意取定的正整数 n 来讨论.

两个整数 a，b 称为模 n 同余，记作

【9.1】
$$a \equiv b(\text{模 } n),$$

如果 n 整除 $b-a$，或如果存在整数 k 使 $b=a+nk$. 容易验证这是一个等价关系. 因而我们可以如在第五节中一样，考虑这个关系定义的等价类，称为模 n 同余类或模 n 剩余类. 用符号 $\bar{a}$ 表示一个整数 a 的同余类. 它是整数的集合

【9.2】
$$\bar{a}=\{\cdots,a-2n,a-n,a,a+n,a+2n,\cdots\}.$$

如果 a，b 是整数，等式 $\bar{a}=\bar{b}$ 是指 n 整除 $b-a$.

0 的同余类是由所有 n 的倍数组成的加法群 $\mathbb{Z}^+$ 的子群

$$\bar{0}=n\mathbb{Z}=\{\cdots,-n,0,n,2n,\cdots\}.$$

其他同余类是这个子群的陪集. 可是，这里的记号有点问题，因为记号 $n\mathbb{Z}$ 看起来像是我们用来表示陪集的符号. 但 $n\mathbb{Z}$ 不是陪集，它是 $\mathbb{Z}^+$ 的子群. 子群 H 的陪集的记号与(6.1)中一样，但合成法则用加号表示，也就是

$$a+H=\{a+h \mid h\in H\}.$$

为避免将陪集写为 $a+n\mathbb{Z}$，将子群 $n\mathbb{Z}$ 记作 H. 则 H 的陪集是集合

【9.3】
$$a+H=\{a+nk \mid k\in \mathbb{Z}\}.$$

它们是同余类 $\bar{a}=a+H$.

n 个整数 0，1，…，$n-1$ 构成同余类的代表元素的一个自然的集合：

【9.4】命题 *模 n 的同余类有 n 个，即*

$$\bar{0},\ \bar{1},\ \cdots,\ \overline{n-1}.$$

64 *或者说，$\mathbb{Z}$ 中的子群 $n\mathbb{Z}$ 的指标 $[\mathbb{Z}:n\mathbb{Z}]$ 是 n.*

证明 设 a 是一个任意整数. 用带余除法，我们记

$$a=nq+r,$$

其中 q，r 是整数并且余数 r 属于 $0\leqslant r<n$ 的范围. 于是 a 与余数同余：$a\equiv r(\text{模 } n)$. 这样 $\bar{a}=\bar{r}$. 这表明 $\bar{a}$ 是命题所列的同余类之一. 另一方面，若 a 和 b 是小于 n 的不同整数，比如说 $a<b$，则 $b-a$ 小于 n 且不等于 0，因而 n 不能整除 $b-a$. 这样 $a\not\equiv b(\text{模 } n)$，这表明 $\bar{a}\neq\bar{b}$. 因此 n 个类 $\bar{0}$，$\bar{1}$，…，$\overline{n-1}$ 互不相同. ■

同余类的要点是模 n 同余保持整数的加法和乘法，因而这些法则可用来定义同余类的加法和乘法. 这可以表述为同余类的集合构成一个环. 我们将在第十章学习环.

设 $\bar{a}$ 和 $\bar{b}$ 是由整数 a 和 b 代表的同余类. 它们的和定义为 $a+b$ 的同余类，它们的积定义为 ab 的类. 换言之，我们定义

【9.5】
$$\bar{a}+\bar{b}=\overline{a+b} \quad \text{和} \quad \bar{a}\bar{b}=\overline{ab}.$$

这个定义需要验证，因为同一个同余类 $\bar{a}$ 可以由许多不同的整数代表. 任一个与 a 模 n 同余的整数 a' 代表同一个类. 因此最好是当 $a'\equiv a$ 且 $b'\equiv b$ 时，$a'+b'\equiv a+b$ 和 $a'b'\equiv ab$ 都成立. 幸运的是，它们的确是成立的.

【9.6】引理 *如果 $a'\equiv a$ 且 $b'\equiv b(\text{模 } n)$，则 $a'+b'\equiv a+b(\text{模 } n)$ 和 $a'b'\equiv ab(\text{模 } n)$.*

证明 假设 $a'\equiv a$ 且 $b'\equiv b$，于是 $a'=a+nr$ 且 $b=b'+ns$ 对某整数 r，s 成立. 从而 $a'+b'=a+b+n(r+s)$，这表明 $a'+b'\equiv a+b$. 类似地，$a'b'=(a+nr)(b+ns)=ab+n(as+rb+nrs)$，

这表明 $a'b'\equiv ab$，正是所要证明的. ■

结合律、交换律和分配律对合成法则(9.5)成立，这是因为它们对整数的加法和乘法是成立的. 例如，分配律的验证如下：

$$\begin{aligned}\bar{a}(\bar{b}+\bar{c}) &= \bar{a}(\overline{b+c}) = \overline{a(b+c)} \quad (\text{同余类}+\text{和}\times\text{的定义})\\ &= \overline{ab+ac} \quad (\text{整数的分配律})\\ &= \overline{ab}+\overline{ac} = \bar{a}\bar{b}+\bar{a}\bar{c} \quad (\text{同余类}+\text{和}\times\text{的定义})\end{aligned}$$

模 n 同余类的集合通常记作

【9.7】

$$\mathbb{Z}/n\mathbb{Z}.$$

$\mathbb{Z}/n\mathbb{Z}$ 的加、减和乘可以通过先对整数计算，然后取用 n 去除所得的余数而直接得到. 这就是公式(9.5)的含义. 这两个公式表明，将整数 a 变到其同余类 $\bar{a}$ 的映射

65

【9.8】

$$\mathbb{Z}\longrightarrow\mathbb{Z}/n\mathbb{Z}$$

与加法和乘法相容. 因而计算可在整数中进行，而在最后搬回到 $\mathbb{Z}/n\mathbb{Z}$ 上. 然而，这样做的效率不高，因为使用较小的数字运算简单一些. 可通过在做了部分运算后取余数，而保持运算中的数字都很小.

于是，如果 $n=13$，

$$\mathbb{Z}/n\mathbb{Z}=\{\bar{0},\bar{1},\bar{2}\cdots,\overline{12}\},$$

则

$$(\bar{7}+\bar{9})(\overline{11}+\bar{6})$$

可以按 $\bar{7}+\bar{9}=\bar{3}$，$\overline{11}+\bar{6}=\bar{4}$，$\bar{3}\cdot\bar{4}=\overline{12}$ 的顺序计算.

数字上面加横线是很烦人的，因而常被省去. 但要记住下面的规则：

【9.9】 在 $\mathbb{Z}/n\mathbb{Z}$ 中说 $a=b$ 是指 $a\equiv b$(模 n).

第十节 商 群

上节我们看到，整数模 n 的同余类是群 $\mathbb{Z}^+$ 的子群 $n\mathbb{Z}$ 的陪集. 这样同余类的加法定义了这些陪集的集合上的一个合成法则. 本节将指出在任意群 G 的正规子群 N 的陪集上可以定义一个合成法则，还将指出如何将陪集的集合构成一个群，这个群称为商群.

角度之和是一个我们熟悉的商结构的例子. 每一实数表示一个角度，两个实数表示同一个角度，如果它们相差 2π 的整数倍. 这是众所周知的. 这个例子的关键是角度的加法是通过实数的加法定义的. 角度构成的群是商群，其中 $G=\mathbb{R}^+$，而 N 是 2π 的整数倍构成的子群.

我们回忆第八节中引入的记号：如果 A，B 是一个群 G 的子集，则

$$AB=\{ab\mid a\in A,b\in B\}.$$

这称为群 G 的两个子集的积，但在其他地方积可能表示集合 $A\times B$.

【10.1】引理 设 N 是群 G 的一个正规子群，则两个陪集 aN，bN 的积仍是一个陪集，事实上

$$(aN)(bN)=abN.$$

66

证明 注意由(6.18)，$Nb=bN$，且因为 N 是子群，$NN=N$. 于是下面的形式推导证明了引理：

$$(aN)(bN) = a(Nb)N = a(bN)N = abNN = abN.$$ ■

这个引理使我们能够定义两个陪集 C_1，C_2 的乘法，其法则为：C_1C_2 是积集．为计算积陪集，取任意元素 $a\in C_1$ 和 $b\in C_2$，使得 $C_1=aN$ 且 $C_2=bN$．于是 $C_1C_2=abN$ 是含有元素 ab 的陪集．这就是我们在上节中定义同余类加法的方法．

例如，考虑在 $G=\mathbb{C}^\times$ 中单位圆 N 的陪集．我们在第五节中已经看到，它的陪集是同心圆

$$C_r = \{z \mid |z| = r\}.$$

公式(10.1)相当于下列断言：若 $|\alpha|=r$ 而 $|\beta|=s$，则 $|\alpha\beta|=rs$：

$$C_rC_s = C_{rs}.$$

对于(10.1)，N 是 G 的正规子群这个假定是很关键的．如果 H 不是 G 的正规子群，则将存在 H 在 G 中的左陪集 C_1，C_2，其乘积不属于单独一个左陪集．因为说 H 不正规是指存在元素 $h\in H$ 和 $a\in G$ 使 $aha^{-1}\notin H$．所以集合

【10.2】 $$(aH)(a^{-1}H)$$

不包含在任何一个左陪集中．它包含 $a1a^{-1}1=1$，这是 H 中的元素．于是，若集合(10.2)包含在一个陪集之中，则这个陪集必为 $H=1H$．但它还包含元素 $aha^{-1}1$，而这个元素不属于 H．

习惯上用符号

【10.3】 $$G/N = G \text{ 中 } N \text{ 的陪集的集合}$$

表示 G 的正规子群 N 的陪集的集合．这与我们在第九节中引入的记号 $\mathbb{Z}/n\mathbb{Z}$ 是一致的．对于陪集，常用的另一个记号是横线记号：

$$G/N = \overline{G} \quad \text{和} \quad aN = \overline{a},$$

因而 $\overline{a}$ 表示包含 a 的陪集．当要考虑映射

【10.4】 $$\pi: G \longrightarrow \overline{G} = G/N \quad \text{使得} \quad a \rightsquigarrow \overline{a} = aN$$

时，这是自然的．

【10.5】定理 *在上面定义的合成法则下，$\overline{G}=G/N$ 是一个群，且映射 π[见(10.4)]是一个同态，其核为 N．*

G/N 的阶是 N 在 G 中的指标$[G:N]$．

67

【10.6】推论 *群 G 的每个正规子群都是一个同态的核．*

这一推论使得我们能够应用所知道的关于同态的知识来增进对正规子群的理解．

定理(10.5)的证明 首先注意 π 是与合成法则相容的：因为陪集的乘法是由元素的乘法定义的，所以 $\pi(a)\pi(b)=\pi(ab)$．而且，G 中与单位元 1 有相同的象的元素是包含在 N 中的元素：$\overline{1}=1N=N$．$\overline{G}$ 中的群公理由引理(10.7)得到．

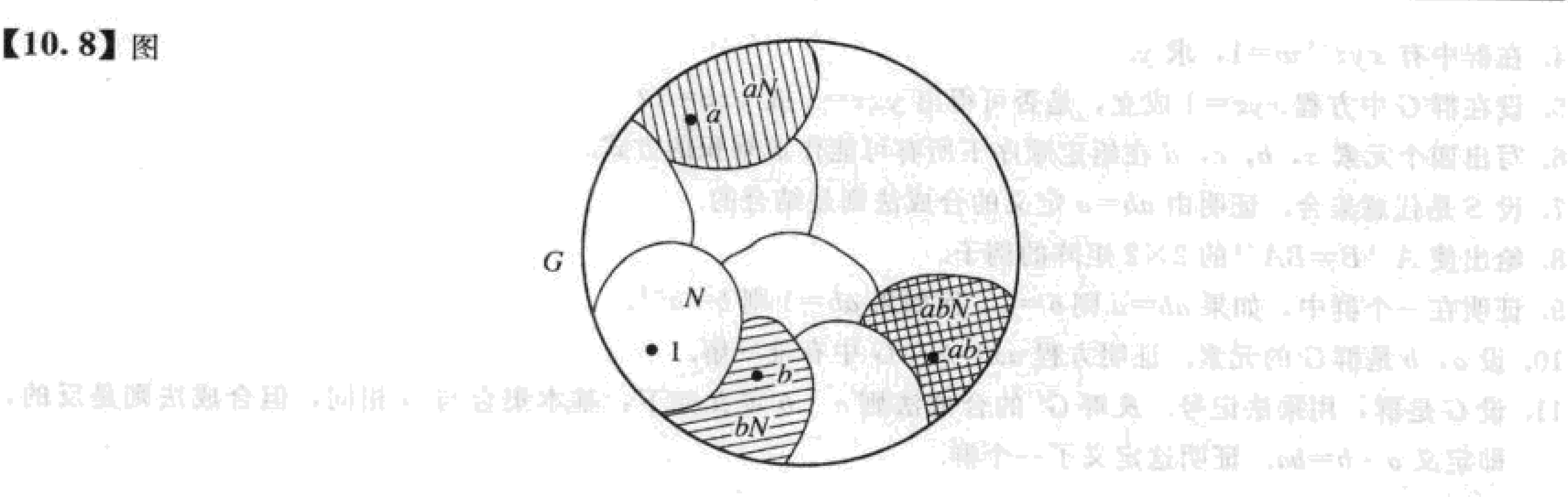
【10.7】引理 *设 G 是群，并且假设 S 是任意有合成法则的集合．设 $\varphi: G\longrightarrow S$ 是一个满射，具有以下性质：对所有 a，b 属于 G，有 $\varphi(a)\varphi(b)=\varphi(ab)$．则 S 是一个群．*

证明 实际上，关于乘法的任何运算法则在 G 中成立，则必在 S 中成立．结合律的证明如下：设 s_1，s_2，$s_3\in S$．因为 φ 是满射，我们知道 $s_i=\varphi(a_i)$ 对某 $a_i\in G$ 成立．于是

$$\begin{aligned}(s_1s_2)s_3 &= (\varphi(a_1)\varphi(a_2))\varphi(a_3) = \varphi(a_1a_2)\varphi(a_3) = \varphi(a_1a_2a_3)\\ &= \varphi(a_1)\varphi(a_2a_3) = \varphi(a_1)(\varphi(a_2)\varphi(a_3)) = s_1(s_2s_3).\end{aligned}$$

其他群公理的证明留作练习． ■

【10.8】图



陪集乘法的示意图

例如，设 $G=\mathbb{R}^{\times}$ 为非零实数的乘法群，且设 P 为正实数的子群. 则有两个陪集，即 P 与 $-P=\{$负实数$\}$，且 $\overline{G}=G/P$ 为二元素群. 乘法法则是熟悉的法则：(负)(负)=(正)，等等.

商群的构造与一般的群同态有如下的联系：

【10.9】定理 第一同构定理：设 $\varphi:G\longrightarrow G'$ 是一个满的群同态，并且设 $N=\ker\varphi$. 则 G/N 与 G' 同构，其同构由将陪集 $\overline{a}=aN$ 映到 $\varphi(a)$ 的映射 $\overline{\varphi}$ 给出：

$$\overline{\varphi}(\overline{a})=\varphi(a).$$

这是我们等同商群的最基本方法. 例如，绝对值映射 $\mathbb{C}^{\times}\longrightarrow\mathbb{R}^{\times}$ 将非零复数映到正实数，其核是单位圆 U. 因而商群 $\mathbb{C}^{\times}/U$ 同构于正实数的乘法群. 另外，行列式是一个满同态 $GL_n(\mathbb{R})\longrightarrow\mathbb{R}^{\times}$，其核为特殊线性群 $SL_n(\mathbb{R})$. 因而商群 $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ 同构于 $\mathbb{R}^{\times}$.

第一同构定理的证明 根据命题(5.13)，φ 的非空纤维是陪集 aN. 因而可以用两种方式考虑 $\overline{G}$，即作为陪集的集合或作为 φ 的非空纤维的集合. 因而我们要找的映射是对集合的任一映射由(5.10)所定义的映射. 它将 $\overline{G}$ 一一地映到 φ 的象上，因为 φ 是满射，这个象等于 G'. 由构造，它与乘法相容：$\overline{\varphi}(\overline{ab})=\varphi(ab)=\varphi(a)\varphi(b)=\overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b})$. ■

有许多种的大小，它们都被神秘的面纱所遮盖；
由此产生了不同的数学分支，
其中每个数学分支研究一种特别的大小.

Leonhard Euler

练　　习

第一节　群的定义

1. (a) 通过直接计算验证(1.17)和(1.18).
   (b) 作出 S_3 的乘法表.
2. (a) 证明 $GL_n(\mathbb{R})$ 是一个群.
   (b) 证明 S_n 是一个群.
3. 设 S 是一个满足结合的合成法则并且有单位元的集合. 证明 S 中由可逆元素组成的子集是一个群.

68

4. 在群中有 $xyz^{-1}w=1$，求 y.
5. 设在群 G 中方程 $xyz=1$ 成立，是否可得出 $yxz=1$ 或 $yzx=1$?
6. 写出四个元素 a，b，c，d 在给定顺序下所有可能作成乘积的方式.
7. 设 S 是任意集合. 证明由 $ab=a$ 定义的合成法则是结合的.
8. 给出使 $A^{-1}B\neq BA^{-1}$ 的 2×2 矩阵的例子.
9. 证明在一个群中，如果 $ab=a$ 则 $b=1$，而如果 $ab=1$ 则 $b=a^{-1}$.
10. 设 a，b 是群 G 的元素. 证明方程 $ax=b$ 在 G 中有唯一解.

69

11. 设 G 是群，用乘法记号. 反群 G° 的合成法则 $a\circ b$ 定义如下：基本集合与 G 相同，但合成法则是反的，即定义 $a\circ b=ba$. 证明这定义了一个群.

第二节 子群

1. 具体确定由矩阵 $\begin{bmatrix}1 & 1\\ -1 & 0\end{bmatrix}$ 所生成的循环群的元素.
2. 设 a，b 是群 G 的元素. 设 a 的阶为 5 且 $a^3b=ba^3$. 证明 $ab=ba$.
3. 下列哪些是子群?
   (a) $GL_n(\mathbb{R})\subset GL_n(\mathbb{C})$.
   (b) $\{1,-1\}\subset\mathbb{R}^{\times}$.
   (c) $\mathbb{Z}^{+}$ 中的正整数集合.
   (d) $\mathbb{R}^{\times}$ 中的正实数集合.
   (e) 所有 $a\neq0$ 的实数矩阵 $\begin{bmatrix}a & 0\\ 0 & 0\end{bmatrix}$ 的集合.
4. 证明对群 G 的非空子集 H，如果对所有 x，$y\in H$，元素 xy^{-1} 也属于 H，则 H 是一子群.
5. 一个 n 次单位根是满足 $z^n=1$ 的复数 z. 证明 n 次单位根构成 $\mathbb{C}^{\times}$ 的 n 阶循环群.
6. (a) 对克莱因四元数群求类似(2.13)的生成元和关系.
   (b) 求克莱因四元数群的所有子群.
7. 设 a，b 为整数.
   (a) 证明子集 $a\mathbb{Z}+b\mathbb{Z}$ 是 $\mathbb{Z}^{+}$ 的子群.
   (b) 证明 a 和 $b+7a$ 生成子群 $a\mathbb{Z}+b\mathbb{Z}$.
8. 作出四元数群 H 的乘法表.
9. 设 H 是由群 G 的两个元素 a，b 生成的子群，证明若 $ab=ba$，则 H 是一个阿贝尔群.
10. (a) 假设一个群的元素 x 的阶为 rs. 求 x^r 的阶.
    (b) 假设 x 的阶为任意的 n，问 x^r 的阶是什么?
11. 证明在任意群中 ab 的阶与 ba 的阶相等.
12. 描述所有没有真子群的群 G.
13. 证明循环群的任意子群是循环群.
14. 设 G 是 n 阶循环群，并设 r 是一个整除 n 的整数. 证明 G 中恰好有一个 r 阶子群.
15. (a) 在子群定义中，要求 H 的单位元是 G 的单位元. 可以只要求 H 有单位元，而不要求它等于 G 的单位元. 证明只要 H 有单位元，则它是 G 的单位元，所以这个定义等价于原来给出的定义.
    (b) 对逆证明类似的结论.
16. (a) 设 G 是 6 阶循环群，它有多少个元素生成 G?
    (b) 对阶为 5，8 和 10 的循环群回答同样的问题.

(c) n 阶循环群有多少个元素是它的生成元?

17. 证明除单位元以外所有元素的阶都是 2 的群是阿贝尔群.

18. 根据第一章(2.18),初等矩阵生成 $GL_n(\mathbb{R})$.

(a) 证明第一类和第三类初等矩阵就足以生成这个群.

(b) 特殊线性群 $SL_n(\mathbb{R})$是行列式为 1 的实 $n\times n$ 矩阵的集合. 证明 $SL_n(\mathbb{R})$是 $GL_n(\mathbb{R})$的子群.

70

*(c) 用行约简证明第一类初等矩阵生成 $SL_n(\mathbb{R})$. 先做 2×2 的情形.

19. 在对称群 S_4 中确定 2 阶元的个数.

20. (a) 设 a, b 是阿贝尔群中阶分别是 m, n 的元素. 对于其积 ab 的阶,有什么结论?

*(b) 举例说明在非阿贝尔群中有限阶元素的乘积未必是有限阶的.

21. 证明阿贝尔群中有限阶元素的集合是一个子群.

22. 证明如文中定义的 a, b 的最大公因子可以通过将 a 和 b 分解成素数的乘积再取公共因子得到.

第三节 同构

1. 证明实数的加法群$\mathbb{R}^+$与正实数的乘法群 P 同构.

2. 证明积 ab 和 ba 在群中是共轭元素.

3. 设 a, b 是群 G 中的元素,且设 $a'=bab^{-1}$. 证明 $a=a'$当且仅当 a 与 b 可交换.

4. (a) 设 $b'=aba^{-1}$. 证明 $b'^n=ab^na^{-1}$.

(b) 证明若 $aba^{-1}=b^2$, 则 $a^3ba^{-3}=b^8$.

5. 设 $\varphi:G\longrightarrow G'$是群的同构. 证明逆函数 φ^{-1}也是一个同构.

6. 设 $\varphi:G\longrightarrow G'$是群的同构,设 x, $y\in G$, 且设 $x'=\varphi(x)$和 $y'=\varphi(y)$.

(a) 证明 x 和 x'的阶相等.

(b) 证明若 $xyx=yxy$, 则 $x'y'x'=y'x'y'$.

(c) 证明 $\varphi(x^{-1})=(x')^{-1}$.

7. 证明矩阵$\begin{bmatrix}1&1\\&1\end{bmatrix}$, $\begin{bmatrix}1&\\1&1\end{bmatrix}$在群 $GL_2(\mathbb{R})$中是共轭的,但它们作为 $SL_2(\mathbb{R})$中的元素时不共轭.

8. 证明矩阵$\begin{bmatrix}1&\\&2\end{bmatrix}$, $\begin{bmatrix}1&3\\&2\end{bmatrix}$在群 $GL_2(\mathbb{R})$中共轭.

9. 求一个群 G 到其反群 G^o(第二节练习 12)的同构.

10. 证明映射 $A \rightsquigarrow (A^t)^{-1}$是 $GL_n(\mathbb{R})$的自同构.

11. 证明群 G 的自同构的集合 Aut$G$ 构成一个群,合成法则为函数的合成.

12. 设 G 是群,并设 $\varphi:G\longrightarrow G$ 是映射 $\varphi(x)=x^{-1}$.

(a) 证明 φ 是一一映射.

(b) 证明 φ 是自同构当且仅当 G 是阿贝尔群.

13. (a) 设 G 是 4 阶群. 证明 G 的每个元素的阶是 1, 2 或 4.

(b) 通过考虑下面两种情形对 4 阶群分类:

(i) G 含有一个 4 阶元素.

(ii) G 的每个元素的阶<4.

14. 确定下列群的自同构群.

(a) $\mathbb{Z}^+$. (b) 10 阶循环群. (c) S_3.

71

15. 证明函数 $f=\frac{1}{x}$, $g=\frac{x-1}{x}$生成一个函数群,合成法则是函数的合成,它同构于对称群 S_3.

16. 给出两个同构的群的例子，它们之间有多于一个同构.

第四节 同态

1. 设 G 为群，合成法则记为 $x \# y$. 设 H 为群，合成法则记为 $u \circ v$. 映射 $\varphi: G \longrightarrow H'$是同态的条件是什么?
2. 设 $\varphi: G \longrightarrow G'$是一个群同态. 证明对 G 的任意元素 $a_1, \cdots, a_k$，$\varphi(a_1 \cdots a_k) = \varphi(a_1) \cdots \varphi(a_k)$.
3. 证明一个同态的核与象是子群.
4. 描述所有同态 $\varphi: \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$，并确定其中哪些是单射，哪些是满射，哪些是同构.
5. 设 G 是一个阿贝尔群. 证明由 $\varphi(x) = x^n$ 定义的 n 次幂映射 $\varphi: G \longrightarrow G$ 是 G 到其自身的同态.
6. 设 $f: \mathbb{R}^+ \longrightarrow \mathbb{C}^\times$ 为映射 $f(x) = e^{ix}$. 证明 f 是同态，并求其核与象.
7. 证明使得 $\alpha \rightsquigarrow |\alpha|$ 的绝对值映射 $|\ |: \mathbb{C}^\times \longrightarrow \mathbb{R}^\times$ 是同态，并求其核与象.
8. (a) 求 S_3 的所有子群，并确定哪些是正规的.

   (b) 求四元数群的所有子群，并确定哪些是正规的.
9. (a) 证明两个同态 φ, ψ 的合成 $\varphi \circ \psi$ 是同态.

   (b) 描述 $\varphi \circ \psi$ 的核.
10. 设 $\varphi: G \longrightarrow G'$是群同态. 证明 $\varphi(x) = \varphi(y)$ 当且仅当 $xy^{-1} \in \ker\varphi$.
11. 设 G, H 是由元素 x, y 生成的循环群. 确定关于 x, y 的阶 m, n 的条件，使得 $x^i \rightsquigarrow y^i$ 的映射是群同态.
12. 证明具有块形式$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$的 $n \times n$ 矩阵 M 构成 $GL_n(\mathbb{R})$ 的子群 P，其中 $A \in GL_r(\mathbb{R})$ 且 $D \in GL_{n-r}(\mathbb{R})$，且使 $M \rightsquigarrow A$ 的映射 $P \longrightarrow GL_r(\mathbb{R})$ 是一同态. 其核是什么?
13. (a) 设 H 是 G 的子群，并设 $g \in G$. **共轭子群** gHg^{-1} 是所有共轭 ghg^{-1} 的集合，其中 $h \in H$. 证明 gHg^{-1} 是 G 的子群.

    (b) 证明 G 的子群 H 是正规的，当且仅当对任意元素 $g \in G$，$gHg^{-1} = H$.
14. 设 N 是 G 的正规子群，且设 $g \in G$，$n \in N$. 证明 $g^{-1}ng \in N$.
15. 设 φ 和 ψ 是群 G 到另一个群 G'的两个同态，且令 $H \subset G$ 为子集$\{x \in G \mid \varphi(x) = \psi(x)\}$. 证明或反证 H 是 G 的子群.
16. 设 $\varphi: G \longrightarrow G'$是群同态，并设 $x \in G$ 是一个 r 阶元素. 对 $\varphi(x)$，有什么结论?

72

17. 证明群的中心是一个正规子群.
18. 证明 $GL_n(\mathbb{R})$ 的中心是子群 $Z = \{cI \mid c \in \mathbb{R}, c \neq 0\}$.
19. 证明如果群中恰有一个 2 阶元素，则这个元素一定含在群的中心中.
20. 考虑形如

$$\begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix}.$$

    的实 3×3 矩阵的集合 U.

    (a) 证明 U 是 $SL_n(\mathbb{R})$ 的子群.

    (b) 证明或反证 U 是正规的.

    *(c) 确定 U 的中心.
21. 通过给出具体例子证明 $GL_2(\mathbb{R})$ 不是 $GL_2(\mathbb{C})$ 的正规子群.
22. 设 $\varphi: G \longrightarrow G'$是群的满同态.

    (a) 设 G 是循环群，证明 G'也是循环群.

    (b) 设 G 是阿贝尔群，证明 G'也是阿贝尔群.

23. 设 $\varphi: G \longrightarrow G'$ 是群的满同态，并设 N 是 G 的正规子群. 证明 $\varphi(N)$ 是 G' 的正规子群.

第五节　等价关系和划分

1. 证明一个映射的非空纤维构成定义域的一个划分.
2. 设 S 是群的集合. 证明关系 $G \sim H$，如果 G 与 H 同构是 S 上的一个等价关系.
3. 确定五个元素的集合上等价关系的个数.
4. 两个等价关系 R，$R' \subset S \times S$ 的交 $R \cap R'$ 是否是等价关系？它们的并呢？
5. 设 H 是群 G 的子群. 证明由规则 $a \sim b$(如果 $b^{-1}a \in H$)定义的关系是 G 上的一个等价关系.
6. (a) 证明群 G 中 x 与 y 共轭是 G 上的一个等价关系.
   (b) 描述其共轭类(等价类)仅有 a 一个元素的元素 a.
7. 设 R 是实数集合 $\mathbb{R}$ 上的一个等价关系. R 可视为 (x, y) 平面的子集. 解释自反性和对称性的几何意义.
8. 对于以下每一个 (x, y)-平面的子集 R，确定 R 满足(5.2)的哪些公理和 R 是否是实数集合 $\mathbb{R}$ 上的一个等价关系？
   (a) $R = \{(s, s) \mid s \in \mathbb{R}\}$.
   (b) R = 空集.
   (c) R = 轨迹 $\{y = 0\}$.
   (d) R = 轨迹 $\{xy + 1 = 0\}$.
   (e) R = 轨迹 $\{x^2y - xy^2 - x + y = 0\}$.
   (f) R = 轨迹 $\{x^2 - xy + 2x - 2y = 0\}$.
9. 描述 (x, y) 平面中包含直线 $x - y = 1$ 的实数集上的最小的等价关系，画出其略图.
10. 画出由 $y = xz$ 定义的 (x, z) 平面到 y 轴的映射的纤维.

73

11. 由整数的法则做出集合(5.8)的加法和乘法法则.
12. 证明陪集(5.14)是映射 φ 的纤维.

第六节　陪集

1. 确定指标 $[\mathbb{Z} : n\mathbb{Z}]$.
2. 直接证明不同的陪集不重叠.
3. 证明每一个阶为素数 p 的幂的群含有一个 p 阶元素.
4. 举例说明 $GL_2(\mathbb{R})$ 在 $GL_2(\mathbb{C})$ 中的左、右陪集不总是相等的.
5. 设 H，K 分别是群 G 的阶为 3，5 的子群. 证明 $H \cap K = \{1\}$.
6. 仔细验证(6.15).
7. (a) 设 G 是奇数阶阿贝尔群. 证明由 $\varphi(x) = x^2$ 定义的映射 $\varphi: G \longrightarrow G$ 是一个自同构.
   (b) 推广(a)的结果.
8. 设 W 是齐次线性方程组 $AX = 0$ 的解组成的 $\mathbb{R}^m$ 的子加法群. 证明非齐次线性方程组 $AX = B$ 的解构成 W 的一个陪集.
9. 设 H 是群 G 的子群. 当(a) G 有限及(b)一般时，证明左陪集的个数等于右陪集的个数.
10. (a) 证明每个指标为 2 的子群是正规的.
    (b) 给出指标为 3 的非正规子群的例子.
11. 通过分析下面三种情形对 6 阶群分类.
    (a) G 含有一个 6 阶元.
    (b) G 含有一个 3 阶元，但没有 6 阶元.
    (c) G 中所有元的阶为 1 或 2.

12. 设 G，H 为 $GL_2(\mathbb{R})$ 的下列子群：

$$G=\left\{\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}\right\},\quad H=\left\{\begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix}\right\}, x>0.$$

G 的元素可以表示为 (x, y) 平面中的点．画出平面作为 H 的左陪集和右陪集的划分．

第七节　限制到子群的同态

1. 设 G，G' 是有限群，其阶无公因数．证明仅有的同态 $\varphi: G \longrightarrow G'$ 是平凡的，即对所有 $x\in G$，$\varphi(x)=1$．
2. 给出一个偶数阶奇置换和一个偶数阶偶置换的例子．
3. (a) 设 H 和 K 是群 G 的子群．证明两个陪集 H 和 K 的交 $xH\cap yK$ 或为空集，或是子群 $H\cap K$ 的陪集．

74

   (b) 证明如果 H 和 K 在 G 中的指标有限，则 $H\cap K$ 的指标有限．
4. 证明命题(7.1)．
5. 设 N，H 是群 G 的子群，且 N 正规．证明 $HN=NH$ 并且这个集合是一个子群．
6. 设 $\varphi: G\longrightarrow G'$ 是群同态，核为 K，并设 H 是 G 的另一子群．用 H 和 K 描述 $\varphi^{-1}(\varphi(H))$．
7. 证明 30 阶的群最多有 7 个 5 阶子群．
*8. 证明*对应定理*：设 $\varphi: G\longrightarrow G'$ 是满的群同态，核为 N．G' 的子群 H' 的集合与 G 的包含 N 的子群 H 的集合间有一个一一对应，对应由映射 $H \rightsquigarrow \varphi(H)$ 和 $\varphi^{-1}(H') \leftsquigarrow H'$ 给出．而且，G 的正规子群对应到 G' 的正规子群．
9. 设 G 和 G' 是分别由 x 和 y 生成的 12 阶和 6 阶群，令 $\varphi: G\longrightarrow G'$ 是由 $\varphi(x^i)=y^i$ 定义的映射．具体列出上题提到的对应．

第八节　群的积

1. 设 G，G' 为群，积群 $G\times G$ 的阶是什么？
2. 对称群 S_3 是非平凡群的直积吗？
3. 证明 rs 阶有限循环群同构于 r 阶和 s 阶循环群的积当且仅当 r 和 s 无公因数．
4. 对下面每一情形，确定 G 是否同构于 H 和 K 的积．
   (a) $G=\mathbb{R}^\times$，$H=\{\pm 1\}$，$K=\{$正实数$\}$．
   (b) $G=\{$可逆上三角 2×2 矩阵$\}$，$H=\{$可逆对角矩阵$\}$，$K=\{$对角线上元素为 1 的上三角矩阵$\}$．
   (c) $G=\mathbb{C}^\times$，$H=\{$单位圆$\}$，$K=\{$正实数$\}$．
5. 证明两个无限循环群的积不是无限循环群．
6. 证明两个群的积的中心是它们的中心的积．
7. (a) 设 H，K 是群 G 的子群．证明积的集合 $HK=\{hk \mid h\in H, k\in K\}$ 是一个子群当且仅当 $HK=KH$．
   (b) 给出一个群 G 和两个子群 H，K，使得 HK 不是子群的例子．
8. 设 G 是群，包含阶分别是 3 和 5 的正规子群．证明 G 包含一个 15 阶元素．
9. 设 G 是有限群，其阶是两个整数的乘积：$n=ab$．设 H，K 分别是群 G 的阶为 a 和 b 的子群．假设 $H\cap K=\{1\}$．证明 $HK=G$．G 同构于积群 $H\times K$ 吗？
10. 设 $x\in G$ 的阶为 m，并设 $y\in G'$ 的阶为 n．问 $G\times G'$ 中元素 (x, y) 的阶是什么？
11. 设 H 是群 G 的子群，并设 $\varphi: G\longrightarrow H$ 为同态，它限制到 H 为恒等映射：$\varphi(h)=h$，如果 $h\in H$．设 $N=\ker\varphi$．
   (a) 证明如果 G 是阿贝尔群，则它同构于积群 $H\times N$．

75

   (b) 不假设 G 是阿贝尔群，找出一个一一映射 $G\longrightarrow H\times N$，但举例说明 G 不必同构于积群．

第九节　模算术

1. 计算 $(7+14)(3-16)$ 模 17．
2. (a) 证明一个整数 a 的平方 a^2 模 4 同余于 0 或 1．

(b) a^2 模 8 可能的值是什么？

3. (a) 证明 2 模 6 没有逆.

   (b) 确定所有使 2 模 n 有一个逆的整数 n.

4. 证明每个整数 a 模 9 同余于其十进制各位数之和.
5. 解同余方程 $2x\equiv5$(a)模 9 和(b)模 6.
6. 确定使同余方程 $x+y\equiv2$，$2x-3y\equiv3$(模 n)有解的整数 n.
7. 对$\mathbb{Z}/n\mathbb{Z}$的乘法证明结合律与交换律.
8. 利用命题(2.6)证明中国剩余定理：设 m，n，a，b 为整数，且设 m，n 的最大公约数是 1，则存在整数 x 使 $x\equiv a$(模 m)且 $x\equiv b$(模 n).

第十节　商群

1. 设 G 是可逆实上三角 2×2 矩阵组成的群. 确定下列条件是否描述 G 的正规子群 H. 如果是，利用第一同构定理确定商群 G/H.

   (a) $a_{11}=1$　(b) $a_{12}=0$　(c) $a_{11}=a_{22}$　(d) $a_{11}=a_{22}=1$

2. 以元素形式写出(10.1)的证明.
3. 设 P 是群 G 的一个划分，具有以下性质：对划分中的任一对元素 A，B，积集 AB 完全包含在划分的另一个元素 C 之中. 设 N 是 P 中包含 1 的元. 证明 N 是 G 的正规子群并且 P 是其陪集的集合.
4. (a) 考虑对称群 S_3 的表示(1.17). 设 H 为子群$\{1, y\}$. 计算积集$(1H)(xH)$和$(1H)(x^2H)$，验证它们不是陪集.

   (b) 证明 6 阶循环群有两个生成元 x，y，满足规则 $x^3=1$，$y^2=1$，$yx=xy$.

   (c) 用(b)替代关系(1.18)重复(a)的计算. 做出解释.

5. 确定商群$\mathbb{R}^\times/P$，其中 P 表示正实数子群.
6. 设 $H=\{\pm1, \pm i\}$是 $G=\mathbb{C}^\times$ 中四次单位根子群. 具体描述 H 在 G 中的陪集，并证明 G/H 同构于 G.
7. 找出四元数群 H 的所有正规子群 N，并确定商群 H/N.
8. 证明行列式为正的矩阵组成的 $G=GL_n(\mathbb{R})$的子集 H 构成一个正规子群，并描述商群 G/H.
9. 证明积群 $G\times G'$的子集 $G\times1$ 是一个与 G 同构的正规子群，且$(G\times G')/(G\times1)$同构于 G'.
10. 描述商群$\mathbb{C}^\times/P$和$\mathbb{C}^\times/U$，其中 U 是绝对值为 1 的复数的子群，而 P 表示正实数.
11. 证明群$\mathbb{R}^+/\mathbb{Z}^+$与$\mathbb{R}^+/2\pi\mathbb{Z}^+$同构.

76

杂题

1. $\mathbb{C}$ 中所有 m 次单位根的积是什么？
2. 计算四元数群的自同构群.
3. 证明偶数阶群含有一个 2 阶元素.
4. 设 $K\subset H\subset G$ 是有限群 G 的子群. 证明公式$[G:K]=[G:H][H:K]$.
5. *半群 S 是具有结合的合成法则和单位元的集合. 但元素不要求有逆，因而消去律不一定成立. 半群 S 称为是由一个元素 s 生成的，如果 s 的非负幂的集合$\{1, s, s^2, \cdots\}$是整个集合 S. 例如，关系 $s^2=1$ 和 $s^2=s$ 刻画了集合$\{1, s\}$上的两个不同的半群结构. 定义半群的同构，并且描述有一个生成元的半群的所有同构类.
6. 若 S 是有有限多个元素的半群且满足消去律(1.12). 证明 S 是群.
7. *设 $a=(a_1, \cdots, a_k)$和 $b=(b_1, \cdots, b_k)$是 k 维空间$\mathbb{R}^k$ 中的点. 从 a 到 b 的一条路是一个$\mathbb{R}^k$ 的$[0, 1]$区间上取值的连续函数，即函数 $f:[0, 1]\longrightarrow\mathbb{R}^k$，使 $t\rightsquigarrow f(t)=(x_1(t), \cdots, x_k(t))$，满足条件 $f(0)=a$ 和$f(1)=b$. 若 S 是$\mathbb{R}^k$ 的子集且 a，$b\in S$，定义 $a\sim b$，如果 a，b 可由一条完全在 S 中的路连起来.

(a) 证明这是 S 上的一个等价关系．注意你构造的路在集合 S 中．

(b) $\mathbb{R}^k$ 的子集 S 称为**路连通的**，如果对任意两点 a，$b\in S$，有 $a\sim b$ 成立．证明 S 的任意子集可由其路连通子集划分，而且不同子集中的两个点不能由 S 中的路连接．

(c) $\mathbb{R}^2$ 中的下列轨道哪些是路连通的？

$\{x^2+y^2=1\}$，$\{xy=0\}$，$\{xy=1\}$．

*8. $n\times n$ 矩阵集合可以等同于空间 $\mathbb{R}^{n\times n}$．设 G 是 $GL_n(\mathbb{R})$ 的子群．证明下列结论．

(a) 如果 A，B，C，$D\in G$，且如果 G 中有 A 到 B 的路和 C 到 D 的路，则 G 中有一条 AC 到 BD 的路．

(b) 可以连到单位矩阵 I 的矩阵集合构成 G 的一个正规子群(称为 G 的**连通分支**)．

*9. (a) 根据 $SL_n(\mathbb{R})$ 由第一类初等矩阵生成(见第二节练习 18)这一事实，证明这个群是路连通的．

(b) 证明 $GL_n(\mathbb{R})$ 是两个路连通子集的并，并描述它们．

10. 设 H，K 是群 G 的子群，并设 $g\in G$．集合

$$HgK=\{x\in G\mid 存在\ h\in H,k\in K\ 使得\ x=hgk\ 成立\}$$

称为**双陪集**．

(a) 证明双陪集划分 G.

(b) 所有双陪集都有相同的阶吗？

11. 设 H 是群 G 的子群．证明若 H 是群 G 的正规子群，则双陪集 HgH 是左陪集 gH，但若 H 不正规，则有真包含左陪集的双陪集．

77

*12. 证明 $GL_n(\mathbb{R})$ 的子群 $H=\{下三角矩阵\}$ 和 $K=\{上三角矩阵\}$ 的双陪集是 HPK，其中 P 是置换矩阵．

第三章　向量空间

> 总是从最简单的例子开始.
>
> *David Hilbert*

第一节　实向量空间

向量空间的基本模型是 n 维行向量或列向量的空间：

$$\mathbb{R}^n\text{:行向量 } v=(a_1,\ \cdots,\ a_n)\text{的集合，或列向量 } v=\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}\text{的集合.}$$

虽然行向量写起来占的空间较少，但矩阵乘法的定义使得列向量对我们更方便．因而多数情况下使用列向量．为了节省空间，我们有时把列向量写成 $(a_1,\ \cdots,\ a_n)^t$ 的形式.

目前我们仅学习两个运算：

【1.1】

$$\text{向量加法：}\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}+\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}=\begin{bmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{bmatrix},$$

$$\text{标量乘法：}c\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}=\begin{bmatrix} ca_1 \\ \vdots \\ ca_n \end{bmatrix}.$$

78

这些运算使 $\mathbb{R}^n$ 成为一个向量空间．在给出向量空间的正式定义之前，我们先看一些其他例子——$\mathbb{R}^n$ 在运算(1.1)下封闭的非空子集．这样的子集称为子空间.

【1.2】例　空间 $\mathbb{R}^2$ 的子空间 W 有三种类型：

(i) 仅有零向量：$W=\{0\}$；

(ii) 位于过原点的直线 L 上的向量；

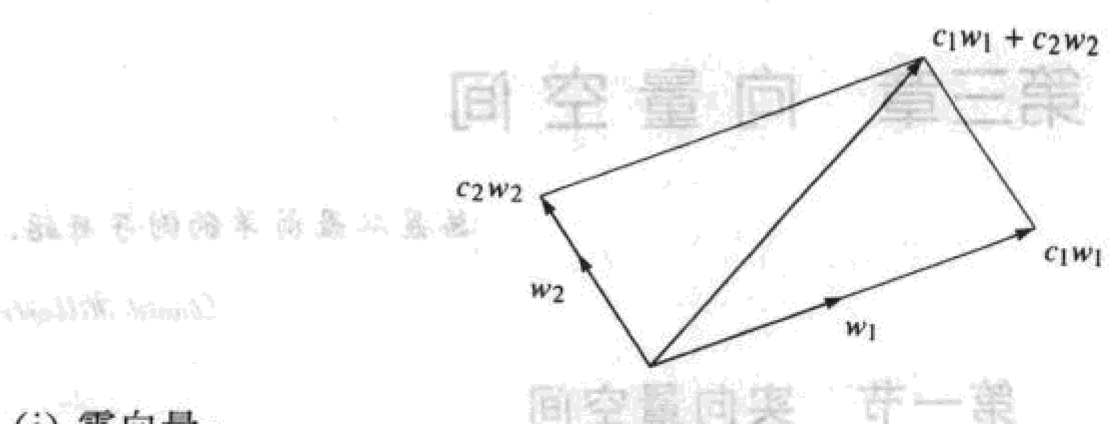
(iii) 整个空间：$W=\mathbb{R}^2$.

这可由向量加法的平行四边形定律看出．若 W 中含有不共线的两个向量 w_1，w_2，则每一向量 v 可由这两个向量"线性组合"得到：

$$c_1w_1+c_2w_2,$$

其中 c_1，c_2 为标量．于是在这种情形有 $W=\mathbb{R}^2$．如果 W 不含有两个这样的向量，则我们得到剩下的两种情形之一.

类似地，可以证明空间 $\mathbb{R}^3$ 的子空间有四种形式：



(i) 零向量；

(ii) 位于过原点的直线上的向量；

(iii) 位于过原点的平面上的向量；

(iv) 整个空间$\mathbb{R}^3$.

$\mathbb{R}^2$ 和$\mathbb{R}^3$ 的子空间的分类将在第四节中通过维数的概念加以解释.

齐次线性方程组衍生出许多例子. 这样的方程组的解的集合总是一个子空间. 这是因为，假如我们用矩阵记号把方程组写为 $AX=0$ 的形式，其中 A 是 $m\times n$ 矩阵而 X 是一个列向量，则显然有

(a) 由 $AX=0$ 和 $AY=0$ 得到 $A(X+Y)=0$. 换言之，若 X，Y 是解，则 $X+Y$ 也是.

79

(b) 由 $AX=0$ 得到 $AcX=0$. 换言之，若 X 是解，则 cX 也是.

例如，设 W 是方程

【1.3】 $$2x_1-x_2-2x_3=0 \quad 或 \quad AX=0, \quad 其中 A=[2 \quad -1 \quad 2]$$

的解. 这个空间是位于过原点且与 A 正交的平面上的向量的集合. 每个解是两个特解 w_1，w_2 的线性组合 $c_1w_1+c_2w_2$. 大多数解对，例如

【1.4】 $$w_1=\begin{bmatrix}1\\0\\1\end{bmatrix}, \quad w_2=\begin{bmatrix}1\\2\\0\end{bmatrix},$$

都将以这种方式张成解空间. 于是每个解都具有形式

【1.5】 $$c_1w_1+c_2w_2=\begin{bmatrix}c_1+c_2\\2c_2\\c_1\end{bmatrix},$$

其中 c_1，c_2 为任意常数. 特解 w_1，w_2 的另一种选择将得到对所有解空间看起来不同但却等价的描述.

【1.6】定义 一个**实向量空间**是具有两个合成法则的集合 V：

(a) 加法：$V\times V\longrightarrow V$，记作 v，$w \rightsquigarrow v+w$.

(b) 标量乘法：$\mathbb{R}\times V\longrightarrow V$，记作 c，$v\rightsquigarrow cv$.

并且这两个合成法则必须满足下列公理：

(i) 加法使 V 成为阿贝尔群 V^+.

(ii) 标量乘法与实数乘法是结合的：

$$(ab)v=a(bv).$$

(iii) 用实数 1 作标量乘法是恒等作用：

$$1v = v.$$

(iv) 两个分配律成立：

$$(a+b)v = av + bv$$

$$a(v+w) = av + aw.$$

当然，所有公理都应加上全称量词，即假设它们对所有 a，$b \in \mathbb{R}$ 及所有 v，$w \in V$ 成立.

V 中加法的单位元记作 0，或者，为了不混淆零向量和数 0，记作 0_V.

80

注意，标量乘法将由实数 c 和向量 v 组成的每对元素对应另一向量 cv. 这样的法则称为向量空间的外部合成法则.

两个向量的乘法不是结构的一部分，虽然可以定义不同的积，如$\mathbb{R}^3$ 中向量的叉积. 这些积不完全是内在的，它们依赖于坐标的选择. 因此将它们看成向量空间上的额外结构.

仔细看一下公理(ii). 左边是指先把 a 和 b 作为实数相乘，然后用 ab 和 v 作标量乘法而得到的向量. 右边两个运算都是标量乘法.

两个合成法则由基本的分配律联系起来. 注意，在第一个分配律中左边的符号+代表实数加法，而在右边则代表向量加法.

【1.7】命题 在一个向量空间 V 中，下列等式成立：

(a) 对所有 $v \in V$，$0_{\mathbb{R}}v = 0_V$.

(b) 对所有 $c \in \mathbb{R}$，$c0_V = 0_V$.

(c) 对所有 $v \in V$，$(-1)v = -v$.

证明 为证(a)，用分配律写出

$$0v + 0v = (0+0)v = 0v = 0v + 0.$$

两边消去 $0v$ 得到 $0v = 0$. 请仔细看一下，注意哪个 0 是数，哪个 0 是向量.

类似地，$c0 + c0 = c(0+0) = c0$，于是 $c0 = 0$. 最后

$$v + -1v = 1v + -1v = (1+-1)v = 0v = 0.$$

因而 $-1v$ 是 v 的加法逆. ■

【1.8】例

(a) $\mathbb{R}^n$ 的子空间是一个这样的向量空间，即它的合成法则由$\mathbb{R}^n$ 上的合成法则导出.

(b) 设 $V = \mathbb{C}$ 是复数集. 忘掉复数乘法，只保持加法 $\alpha + \beta$ 以及复数 α 和实数 c 的乘法 $c\alpha$. 这使得$\mathbb{C}$ 成为实向量空间.

(c) 实多项式 $p(x) = a_n x^n + \cdots + a_1 x + a_0$ 的集合是向量空间，其合成法则为多项式的加法以及标量和多项式的乘法.

(d) 设 V 是区间$[0, 1]$上实值连续函数的集合. 只看函数加法 $f+g$ 以及数与函数的乘法 cf 两个运算. 这使得 V 成为实向量空间.

81

注意，这些例子都有比我们将其视为向量空间更多的结构. 这些是很典型的例子. 每一个例子一定有不同于其他例子的特性，这并不是定义的缺陷. 恰好相反，抽象方法的威力就在于一般公理的结论可用于许多不同的实例.

第二节 抽 象 域

在线性代数中同时处理实的和复的情形是方便的. 这可以通过列出公理化方法所需的“标量”的性质来实现，这样做就产生了域的概念.

过去的惯例是只讲到复数的子域. $\mathbb{C}$ 的子域是在四则运算加、减、乘、除下封闭且包含 1 的任意子集. 换言之，F 是$\mathbb{C}$ 的一个子域，如果下列条件成立：

【2.1】

(a) 若 a，$b\in F$，则 $a+b\in F$.

(b) 若 $a\in F$，则 $-a\in F$.

(c) 若 a，$b\in F$，则 $ab\in F$.

(d) 若 $a\in F$ 且 $a\neq 0$，则 $a^{-1}\in F$.

(e) $1\in F$.

注意，可用公理(a)、(b)和(e)得到 $1-1=0$ 是 F 的一个元. 这样，F 是一个子集，它在加法下是$\mathbb{C}^{+}$ 的子群，而在乘法下 $F\setminus\{0\}=F^{\times}$ 是$\mathbb{C}^{\times}$ 的子群. 反过来，任意这样的子集是子域.

下面是一些$\mathbb{C}$ 的子域的例子：

【2.2】例

(a) $F=\mathbb{R}$，实数域.

(b) $F=\mathbb{Q}$，有理数(即整数的分数)域.

(c) $F=\mathbb{Q}[\sqrt{2}]$，形如 $a+b\sqrt{2}$的复数的域，其中 a，$b\in\mathbb{Q}$.

对最后一个例子，验证公理(2.1)是一个很好的练习.

现在的惯例是抽象地引入域. 抽象域的概念比起$\mathbb{C}$ 的子域更难于掌握，但它包含了重要的新的域类，其中包括有限域.

82

【2.3】定义 域 F 是具有称为加法和乘法的两个合成法则

$$F\times F\xrightarrow{+}F \quad \text{和} \quad F\times F\xrightarrow{\times}F$$
$$a,b\rightsquigarrow a+b \qquad a,b\rightsquigarrow ab$$

并且满足下列公理的集合：

(i) 加法使 F 成为一个阿贝尔群 F^{+}. 其单位元记为 0.

(ii) 乘法是结合和交换的，并且使 $F^{\times}=F-\{0\}$成为一个群. 其单位元记为 1.

(iii) 分配律：对所有 a，b，$c\in F$，$(a+b)c=ac+bc$.

前面两个公理分别描述加法和乘法这两个合成法则. 第三个公理，也就是分配律，是联系加法和乘法的. 这个公理是关键的，因为如果两个合成法则没有联系，就可以分别单独地研究它们. 当然我们知道，实数满足这些公理，但它们就是算术运算所需要的全部公理，这一事实只有在使用它们后才能理解.

读者可以计算其元素属于一个任意域的矩阵. 第一章的讨论可原封不动地重复，应该把这一点牢记在心，再回去看看那些内容.

除复数的子域之外，最简单的域是称为素域的一些有限域，下面就来描述它们. 在第二章

第九节中，我们看到，模 n 同余类的集合$\mathbb{Z}/n\mathbb{Z}$具有由整数的加法和乘法导出的加法和乘法法则．对于整数，除了公理(ii)中乘法逆的存在性以外，域的所有公理都成立．整数对除法不封闭．正如我们前面所指出的，这些公理也延续到了同余类的加法和乘法．但没有理由假定同余类存在乘法逆，事实上逆也不一定存在．例如，类 2 模 6 没有乘法逆．因而，下面的事实是令人惊奇的：若 p 是素数，则所有模 p 非零的同余类皆有逆，这样集合$\mathbb{Z}/p\mathbb{Z}$是域．这个域称为素域，通常记作$\mathbb{F}_p$：

【2.4】
$$\mathbb{F}_p = \{\overline{0},\overline{1},\cdots,\overline{p-1}\} = \mathbb{Z}/p\mathbb{Z}.$$

【2.5】定理 *设 p 是一个素整数．每一个非零同余类 $\overline{a}$(模 p)有乘法逆，因而$\mathbb{F}_p$是有 p 个元素的域．*

定理也可以叙述为：

【2.6】 *设 p 是素数，并设 a 是不能被 p 整除的任意整数．则有整数 b 使得 $ab\equiv 1$(模 p)．*

83

因为 $ab\equiv 1$(模 p)和 $\overline{a}\,\overline{b}=\overline{ab}=\overline{1}$是同一回事，这说明$\overline{b}$是 $\overline{a}$ 的乘法逆．

例如，设 $p=13$ 而 $\overline{a}=\overline{6}$．则 $\overline{a}^{-1}=\overline{11}$，因为

$$6\cdot 11 = 66 \equiv 1(\text{模 } 13).$$

一般来说，求同余类 $\overline{a}$(模 p)的逆并不容易，但当 p 不大时，可以通过反复试验找到．一个系统的方法是计算 $\overline{a}$ 的幂．每一个非零同余类都有逆，所有非零同余类构成一个阶为 $p-1$ 的有限群，通常记作$\mathbb{F}_p^{\times}$．从而每个元 $\overline{a}$ 的阶有限且整除 $p-1$．这样，如果 $p=13$ 而 $\overline{a}=\overline{3}$，我们求得 $\overline{a}^2=\overline{9}$，而 $\overline{a}^3=\overline{27}=\overline{1}$，这表明 $\overline{a}$ 的阶为 3．我们幸运地得到：$\overline{a}^{-1}=\overline{a}^2=\overline{9}$．另一方面，如果用$\overline{a}=\overline{6}$来试的话，会发现$\overline{6}$的阶是 12．这样计算将会很长．

定理(2.5)的证明 设 $\overline{a}\in\mathbb{F}_p$ 是任意非零元，我们用刚刚讨论的方法证明 $\overline{a}$ 有逆．考虑幂 1，$\overline{a}$，$\overline{a}^2$，$\overline{a}^3$，$\cdots$．因为有无限多个幂而$\mathbb{F}_p$ 中仅有有限多个元素，所以必有两个幂是相等的，比如说 $\overline{a}^m=\overline{a}^n$，其中 $m<n$．在这里，我们想要消去 $\overline{a}^m$ 而得到$\overline{1}=\overline{a}^{n-m}$．一旦证明了消去律成立，就将证明 $\overline{a}^{n-m-1}$是 $\overline{a}$ 的逆．同时也将完成证明．

下面是我们需要的消去律．

【2.7】引理 *消去律：设 $\overline{a}$，$\overline{c}$，$\overline{d}$ 是$\mathbb{F}_p$ 的元素且 $\overline{a}\neq\overline{0}$．如果 $\overline{a}\overline{c}=\overline{a}\,\overline{d}$，则 $\overline{c}=\overline{d}$．*

证明 取$\overline{b}=\overline{c}-\overline{d}$．这时引理的断言变成：如果 $\overline{a}\,\overline{b}=\overline{0}$且 $\overline{a}\neq 0$，则$\overline{b}=\overline{0}$．为证明这一点，我们用整数 a，b 代表同余类 $\overline{a}$，$\overline{b}$．则所要证的是下面这个直观上很容易接受的事实：

【2.8】引理 *设 p 是素数而 a，b 是整数．如果 p 整除积 ab，则 p 整除 a 或 p 整除 b．*

证明 设 p 不整除 a，但 p 整除 ab．我们必须证明 p 整除 b．因为 p 是素数，整除它的正整数只有 1 和 p．因为 p 不整除 a，所以 p 和 a 仅有的公因数为 1．从而 1 是它们的最大公因数．由第二章的命题(2.6)，存在整数 r，s 使 $1=rp+sa$．两边乘 b：$b=rpb+sab$．这个等式右边的两项都可被 p 整除，因而其左边 a 也可被 p 整除，这正是所要证明的． ■

一般来说，与同余一样，域$\mathbb{F}_p$ 的计算也可以通过整数来进行，除了除法以外．这一困难可以这样克服，即把所有的运算都放在一个公分母上进行，而将要做的除法留到最后．例如，假如要在域$\mathbb{F}_p$ 中求解 n 个有 n 个变量的线性方程的方程组．以合适的方式选择剩余类的代表，将方程组用一个整数方程组表出．设整数方程组为 $AX=B$，其中 A 是一个 $n\times n$ 整数矩阵，而 B 是一个整数列向量．要在$\mathbb{F}_p$ 中解方程组，我们设法模 p 求矩阵 A 的逆．用克拉默法则，

84

$(\mathrm{adj}A)A=\delta I$，其中 $\delta=\det A$，这个公式对整数成立[第一章(5.7)]，因而当矩阵元素由其同余类代替时，在$\mathbb{F}_p$中也成立. 若 δ 的剩余类非零，则可以通过计算 $\delta^{-1}(\mathrm{adj}A)$在$\mathbb{F}_p$中求 A 的逆.

【2.9】推论 考虑 n 个有 n 个未知量的线性方程的方程组 $AX=B$，其中 A，B 的元素属于$\mathbb{F}_p$. 如果在$\mathbb{F}_p$中 $\det A\neq 0$，则方程组在$\mathbb{F}_p$中有唯一解.

例如，考虑线性方程组 $AX=B$，其中

$$A=\begin{bmatrix}8 & 3\\ 2 & 6\end{bmatrix} \quad 和 \quad B=\begin{bmatrix}3\\ -1\end{bmatrix}.$$

因为系数是整数，对任意素数 p，它们定义$\mathbb{F}_p$上的一个方程组. A 的行列式是 42，故当 p 不是 2，3 和 7 时，方程组在$\mathbb{F}_p$中有唯一解. 这样，若 $p=13$，当(模 13)取值时，得到 $\det A=3$. 我们已经看到在$\mathbb{F}_{13}$中 $3^{-1}=9$. 因此，可用克拉默法则计算得到

$$在\mathbb{F}_{13}中\ A^{-1}=\begin{bmatrix}2 & -1\\ 8 & 7\end{bmatrix} \quad 和 \quad X=A^{-1}B=\begin{bmatrix}7\\ 4\end{bmatrix}.$$

方程组在$\mathbb{F}_2$或$\mathbb{F}_3$中无解，但在$\mathbb{F}_7$中碰巧有解，虽然在这个域中 $\det A=0$.

顺便指出，元素属于$\mathbb{F}_p$的可逆矩阵为我们提供了有限群的新例子——有限域上的一般线性群：

$$GL_n(\mathbb{F}_p)=\{元素属于\mathbb{F}_p的\ n\times n\ 可逆矩阵\}.$$

其中，最小的是元素为(模 2)的剩余类组成的 2×2 可逆矩阵的群 $GL_2(\mathbb{F}_2)$，它由六个矩阵组成：

【2.10】

$$GL_2(\mathbb{F}_2)=\left\{\begin{bmatrix}1 & \\ & 1\end{bmatrix},\begin{bmatrix} & 1\\ 1 & \end{bmatrix},\begin{bmatrix}1 & 1\\ & 1\end{bmatrix},\begin{bmatrix}1 & 1\\ 1 & \end{bmatrix},\begin{bmatrix}1 & \\ 1 & 1\end{bmatrix},\begin{bmatrix} & 1\\ 1 & 1\end{bmatrix}\right\}.$$

有限域 $F=\mathbb{F}_p$ 有一个性质，它使有限域与$\mathbb{C}$的子域区别开来并且有时影响到计算. 这个性质就是 1 自己相加若干次后(事实上是 p 项)得到 0. 域 F 称为具有特征 p，如果在 F 中$1+\cdots+1$(p 项)$=0$，并且 p 是具有这一性质的最小正整数. 换句话说，如果作为加法群 F^+ 的一个元素，1 的阶是有限的话，F 的特征是这个阶(第二章第二节). 如果 1 的阶是无限的，即在 F 中$1+\cdots+1$从不为 0，则我们说域 F 有特征零，这看起来似乎有点自相矛盾. 这样$\mathbb{C}$的子域有特征零，而素域$\mathbb{F}_p$有特征 p. 可以证明，任何域的特征或者为零，或者为一个素数. [85]

现在设 F 是一个任意域. 域 F 上的向量空间和(1.6)一样定义，只是用 F 来代替$\mathbb{R}$.

【2.11】定义 域 F 上的一个向量空间是具有两个合成法则的集合：

(a) 加法：$V\times V\longrightarrow V$，记为 $v,w\rightsquigarrow v+w$，

(b) 标量乘法：$F\times V\longrightarrow V$，记为 $c,v\rightsquigarrow cv$，

并且这两个合成法则满足下列公理：

(i) 加法使 V 成为阿贝尔群 V^+.

(ii) 标量乘法与 F 中的乘法是结合的：

$$(ab)v=a(bv),\quad 对所有\ a,b\in F\ 和\ v\in V.$$

(iii) 元素 1 的作用是恒等作用：$1v=v$，对所有 $v\in V$.

(iv) 两个分配律成立：

$$(a+b)v=av+bv \quad 和 \quad a(v+w)=av+aw,$$

对所有 $a, b\in F$ 和 $v\in V$.

第一节的一切都可将$\mathbb{R}$换成 F 复述. 这样行向量$(a_1, \cdots, a_n)(a_i\in F)$的空间 F^n 是 F 上的向量空间，等等.

重要的是注意向量空间的定义隐含了域 F 的选择. 域 F 中的元素常称为标量. 我们通常保持这个域不变. 当然，如果 V 是复向量空间，也就是域$\mathbb{C}$上的向量空间，且 $F\subset\mathbb{C}$ 是任意子域，则 V 自然也是一个 F 上的向量空间，因为 cv 对所有的 $c\in F$ 都有定义. 但当把标量乘法由$\mathbb{C}$限制到 F 时，我们认为向量空间结构已发生了变化.

与群的子群和同构类似的两个重要概念是子空间和向量空间同构. 对复向量空间我们已经定义了子空间，而这个定义对任意域都是一样的. (域 F 上的)向量空间 V 的子空间 W 是具有下列性质的子集：

【2.12】

(a) 若 $w, w'\in W$，则 $w+w'\in W$.

(b) 若 $w\in W$ 且 $c\in F$，则 $cw\in W$.

(c) $0\in W$.

86

子空间 W 称为 V 的一个真子空间，如果它既不是整个空间 V，也不是零空间$\{0\}$.

容易看出，子空间就是这样一个子集，合成法则在其上导出向量空间的结构.

如同第一节一样，m 个有 n 个未知量而系数属于 F 的线性方程的方程组

$$AX=0$$

的所有解的空间，是空间 F^n 的一个子空间的例子.

【2.13】定义 在同一个域 F 上，一个向量空间 V 到另一个向量空间 V'的**同构** φ 是一个与合成法则相容的一一映射 $\varphi: V\longrightarrow V'$，即对所有 $v, v'\in V$ 及所有 $c\in F$ 满足条件

$$\text{(a) } \varphi(v+v')=\varphi(v)+\varphi(v') \quad \text{和} \quad \text{(b) } \varphi(cv)=c\varphi(v)$$

的一一映射.

【2.14】例

(a) n 维行向量空间与 n 维列向量空间同构.

(b) 将复数$\mathbb{C}$如(1.8b)一样视为实向量空间，则使$(a, b)\rightsquigarrow a+bi$ 的映射 $\varphi: \mathbb{R}^2\longrightarrow\mathbb{C}$ 是一个同构.

第三节 基和维数

本节讨论在一个抽象地给出的向量空间中，当使用加法和标量乘法时所用的术语. 新的概念有张成、线性无关和基.

这里使用向量的有序集会很方便. 大部分情形序都将是不重要的，但在进行精确计算时，它以一种很本质的方式进入运算的过程. 我们已将无序集用花括号括起来表示，为了区别有序集和无序集，将有序集用圆括号括起来表示. 这样有序集(a, b)和(b, a)是不同的，而无序集$\{a, b\}$和$\{b, a\}$是相同的. 有序集允许重复. 这样(a, a, b)是一个有序集，且它与(a, b)不同，这与无序集的习惯不同，无序集$\{a, a, b\}$和$\{a, b\}$表示同一个集合.

设 V 是域 F 上的一个向量空间，$(v_1, \cdots, v_n)$是 V 中元素的有序集．$(v_1, \cdots, v_n)$的线性组合是形如

87 【3.1】
$$w = c_1v_1 + c_2v_2 + \cdots + c_nv_n, \quad c_i \in F$$
的任意向量.

例如，设有序集由(1.4)中考虑的两个向量 $v_1=(1, 0, 1)^t$ 和 $v_2=(1, 2, 0)^t$ 组成．则线性组合将具有(1.5)的形式：$(c_1+c_2, 2c_2, c_1)^t$．向量$(3, 4, 1)^t=v_1+2v_2$ 就是一个这样的线性组合.

写为矩阵形式的线性方程组 $AX=B$[第一章(1.9)]的一个解 X 把列向量 B 写成了矩阵 A 的列向量的线性组合．系数是向量 X 的元素.

单独一个向量(v)的线性组合就是 v 的倍数 cv.

可以写成$(v_1, \cdots, v_n)$的线性组合的所有向量 w 的集合构成 V 的子空间 W，称为由该集合张成的向量空间：若 w 如(3.1)给出，而 $w'=c'_1v_1+c'_2v_2+\cdots+c'_nv_n$ 是 W 的元，则
$$w + w' = (c_1 + c'_1)v'_1 + (c_2 + c'_2)v'_2 + \cdots + (c_n + c'_n)v_n$$
也是，且如果 $a\in F$，则 $aw=(ac_1)v_1+(ac_2)v_2+\cdots+(ac_n)v_n$ 也属于 W．于是 $w+w'$ 和 aw 属于 W．最后，$0=0v_1+0v_2+\cdots+0v_n\in W$．这表明(2.12)的条件成立.

由集合 S 张成的空间常记为 Span$S$．Span$S$ 无疑是 V 的包含 S 的最小子空间．我们也可将它称为由 S 生成的子空间．注意，这里序是无关紧要的．S 的张成与 S 的任意重排序的张成是相同的.

我们也可以定义向量的无限集合的张成，这将在第五章中讨论．本节假设集合是有限的.

【3.2】命题 设 S 是 V 中的向量的集合，并设 W 是 V 的一个子空间．若 $S\subset W$，则 Span$S\subset W$.

这是显然的，因为 W 关于加法和标量乘法封闭．若 $S\subset W$，则 S 的任何向量的线性组合也包含在 W 中.

向量 $v_1, \cdots, v_n$ 间的线性关系是形如

【3.3】
$$c_1v_1 + c_2v_2 + \cdots + c_nv_n = 0$$
的任意关系，其中系数 c_i 属于 F．向量的一个有序集$(v_1, \cdots, v_n)$称为**线性无关的**，如果除了系数皆为零的平凡关系外，这个集合的向量间没有其他线性关系．正面地叙述这个条件是很有用的：

【3.4】 设$(v_1, \cdots, v_n)$是线性无关的集合．则对方程 $c_1v_1+\cdots+c_nv_n=0$，可以得到对 $i=1, \cdots, n$，$c_i=0$.

反之，若(3.4)成立，则向量线性无关.

88 向量(1.4)是线性无关的.

注意，线性无关集 S 不能有任何重复，因为如果 S 中的向量 v_i，v_j 相等，则
$$v_i - v_j = 0$$
是一个形如(3.3)的线性关系，其他的系数都是零．另外，线性无关族中没有向量可以是零，因为 $v_i=0$ 是一个线性关系.

不是线性无关的集合称为是**线性相关的**.

如果 V 是空间 F^m，且向量$(v_1, \cdots, v_n)$已具体给出，则可以通过解一个齐次线性方程组来确定其线性相关性. 因为说线性组合 $x_1v_1+\cdots+x_nv_n$ 为零意味着它的每个分量都为零，这给出 n 个未知量 x_i 的 m 个方程. 例如，考虑三个向量的集合

【3.5】
$$v_1=\begin{bmatrix}1\\0\\1\end{bmatrix},\quad v_2=\begin{bmatrix}1\\2\\0\end{bmatrix},\quad v_3=\begin{bmatrix}2\\1\\2\end{bmatrix}.$$

用 A 表示列为这些向量的矩阵

【3.6】
$$A=\begin{bmatrix}1&1&2\\0&2&1\\1&0&2\end{bmatrix}.$$

这些向量的一般线性组合具有 $x_1v_1+x_2v_2+x_3v_3$ 的形式. 将标量系数写到另一边，可将这个线性组合写为 AX 的形式，其中 $X=(x_1, x_2, x_3)^t$. 因为 $\det A=1$，方程 $AX=0$ 只有平凡解，这证明了(v_1, v_2, v_3)是线性无关集合. 另一方面，在这个集合上添加任意第四个向量 v_4，结果是线性相关的，因为每一个有四个变量的三个齐次方程的方程组有非平凡解[第一章(2.17)].

下面是关于线性无关的一些基本事实.

【3.7】命题

(a) 线性无关集合在任意重新排序后仍是线性无关集合.

(b) 若 $v_1\in V$ 是非零向量，则集合(v_1)线性无关.

(c) 两个向量的集合(v_1, v_2)线性相关当且仅当或者 $v_1=0$，或者 v_2 是 v_1 的倍数.

我们检验断言中的第三条：假设(v_1, v_2)线性相关. 设其关系是 $c_1v_1+c_2v_2=0$，其中 c_1，c_2 不全为零. 若 $c_2\neq 0$，我们可对 v_2 求解：

$$v_2=\frac{-c_1}{c_2}v_1.$$

89

此时 v_2 是 v_1 的倍数. 若 $c_2=0$，则 $c_1\neq 0$ 并且方程表明 $v_1=0$. 反之，若 $v_2=cv_1$，则关系 $cv_1-v_2=0$ 表明集合(v_1, v_2)是线性相关的，且如果 $v_1=0$ 则关系 $v_1+0v_2=0$ 表明同样的结论.

线性无关且张成 V 的一个向量集合$(v_1, \cdots, v_n)$称为一个基. 例如，向量(1.4)构成线性方程(1.3)的解空间的一个基. 我们常用如 $\boldsymbol{B}$ 这样的记号表示一个基.

设 $\boldsymbol{B}=(v_1, \cdots, v_n)$是一个基. 则因为 $\boldsymbol{B}$ 张成 V，每一 $w\in V$ 可以写为一个线性组合(3.1). 因为 $\boldsymbol{B}$ 是线性无关的，所以这个表达式是唯一的.

【3.8】命题　集合 $\boldsymbol{B}=(v_1, \cdots, v_n)$是基当且仅当每个向量 $w\in V$ 可以以唯一方式写为(3.1)的形式.

证明　设 $\boldsymbol{B}$ 是基，且 w 可以以两种方式写为线性组合，比如说(3.1)和 $w=c'_1v_1+\cdots+c'_nv_n$. 则

$$0=w-w=(c_1-c'_1)v_1+\cdots+(c_n-c'_n)v_n.$$

因此，由(3.4)得 $c_1-c'_1=0, \cdots, c_n-c'_n=0$. 这样，两个线性组合是相同的. 另一方面，$\boldsymbol{B}$ 线性无关的定义可以重新叙述为 0 仅有一个作为线性组合的表达式. 这就证明了其逆. ■

【3.9】例　设 $V=F^n$ 是列向量空间，且设 e_i 表示在第 i 个位置为 1 而其他位置为 0 的列向量. n 个向量 e_i 组成 F^n 的一个基，称为标准基. 这个基在前面第一章第四节就已引入. 我们将它

记为 $\mathbf{E}$. 每个向量 $X=(x_1, \cdots, x_n)^t$ 作为 $\mathbf{E}=(e_1, \cdots, e_n)$的线性组合有唯一表达式

$$\mathbf{X}=x_1e_1+\cdots+x_ne_n.$$

集合(3.5)是$\mathbb{R}^3$ 的另一个基.

我们现在讨论主要事实(3.15)～(3.17)，它们将张成、线性无关和基三个概念联系起来.

【3.10】命题 设 L 是 V 中的一个线性无关有序集，$v\in V$ 是任一向量. 则由将 v 加到 L 上得到的有序集 $L'=(L, v)$线性无关当且仅当 v 不属于 L 张成的子空间.

证明 设 $L=(v_1, \cdots, v_r)$. 若 $v\in \operatorname{Span} L$，则对 $c_i\in F$，$v=c_1v_1+\cdots+c_rv_r$ 成立. 因而

90

$$c_1v_1+\cdots+c_rv_r+(-1)v=0$$

是 L'的向量间的线性关系且系数(−1)非零. 这样 L'线性相关.

反之，设 L'线性相关，则存在线性关系

$$c_1v_1+\cdots+c_rv_r+bv=0,$$

其中不是所有系数都为零. 于是必有 $b\neq 0$. 因为若 b 为零，则表达式化为

$$c_1v_1+\cdots+c_rv_r=0.$$

因为 L 线性无关，我们也可得到 $c_1=\cdots=c_r=0$，与假定矛盾. 既然有 $b\neq 0$，就可解出 v：

$$v=\frac{-c_1}{b}v_1+\cdots+\frac{-c_r}{b}v_r.$$

这样 $v\in \operatorname{Span}L$. ■

【3.11】命题 设 S 是向量的有序集，设 $v\in V$ 是任意向量且设 $S'=(S, v)$. 则 $\operatorname{Span}S=\operatorname{Span}S'$当且仅当$v\in \operatorname{Span}S$.

证明 由定义 $v\in \operatorname{Span}S'$. 因而，若 $v\notin \operatorname{Span}S$，则 $\operatorname{Span}S\neq\operatorname{Span}S'$. 反之，若 $v\in \operatorname{Span}S$，则 $S'\subset\operatorname{Span}S$. 因此，$\operatorname{Span}S'\subset\operatorname{Span}S$[由命题(3.2)]. 而事实上 $\operatorname{Span}S'\supset\operatorname{Span}S$ 是平凡的，所以 $\operatorname{Span}S'=\operatorname{Span}S$. ■

【3.12】定义 向量空间 V 称为**有限维的**，如果存在有限集合 S，它张成 V.

在本节余下部分，我们假设向量空间 V 是有限维的.

【3.13】命题 任意张成 V 的有限集 S 包含一个基，特别地，任意有限维向量空间有基.

证明 设 $S=(v_1, \cdots, v_n)$不是线性无关的. 则存在线性关系

$$c_1v_1+\cdots+c_nv_n=0,$$

其中某个 c_i 不为零，不妨设 $c_n\neq 0$. 则我们可解出 v_n：

$$v_n=\frac{-c_1}{c_n}v_1+\cdots+\frac{-c_{n-1}}{c_n}v_{n-1}.$$

这表明 $v_n\in \operatorname{Span}(v_1, \cdots, v_{n-1})$. 在(3.11)中，取 $v=v_n$ 和 $S=(v_1, \cdots, v_{n-1})$，我们得到 $\operatorname{Span}(v_1, \cdots, v_{n-1})=\operatorname{Span}(v_1, \cdots, v_n)=V$. 因而，可以从 S 中去掉 v_n. 这样继续下去，最终得到一个线性无关集族且它仍张成 V，即它是一个基.

91

注意 如果 V 是零向量空间{0}，这个证明会出问题. 因为从 V 中的任何一组向量

(它们全部都等于零)开始，我们的过程会将它们一次一个地丢掉，直到只剩下一个向量 $v_1=0$. 而(0)是线性相关集合. 我们如何把它去掉？当然，零向量空间并不特别有意义. 但它会藏在某个地方，等待我们踏进它的陷阱. 我们必须允许在诸如解齐次线性方程组的某些运算过程中出现的向量空间可能是零空间. 为了避免今后需要把这种情形特别提出来，我们采用下面的约定.

【3.14】

(a) 空集线性无关.

(b) 空集的张成是零子空间.

这样，空集是零向量空间的基. 这个约定使我们能够扔掉最后一个向量 $v_1=0$，这样证明就不会出问题了.

【3.15】命题 设 V 是有限维向量空间. 任意线性无关集 L 可通过添加元素而扩张成一个基.

证明 设 S 是张成 V 的一个有限集. 若 S 的所有元素属于 $\mathrm{Span}L$，则 L 张成 V[(3.2)]，因而它是一个基. 否则，取不属于 $\mathrm{Span}L$ 的元 $v\in S$. 由(3.10)，(L, v)线性无关. 继续下去直到得到一个基. ■

【3.16】命题 设 S，L 是 V 的有限子集，S 张成 V 而 L 线性无关. 则 S 所含元素个数至少与 L 的一样多.

证明 为证明这一点，我们用集 S 写出 L 的线性相关关系，得到有 n 个未知量的 m 个齐次线性方程的方程组，其中 $m=|S|$，$n=|L|$. 设 $S=(v_1, \cdots, v_m)$而 $L=(w_1, \cdots, w_n)$. 我们将每个向量 w_j 写成 S 的线性组合，这样做是因为 S 张成 V，比如

$$w_j = a_{1j}v_1 + \cdots + a_{mj}v_m = \sum_i a_{ij}v_i.$$

设 $u=c_1w_1+\cdots+c_nw_n=\sum_j c_jw_j$ 是线性组合，代入 w_j 得到

$$u = \sum_{i,j} c_j a_{ij} v_i.$$

这个和中 v_i 的系数是 $\sum_j a_{ij}c_j$. 如果对所有 i 这个系数为零，则 $u=0$. 因而要得到 L 的向量间的线性关系，只要解有 n 个未知量的 m 个方程的方程组 $\sum_j a_{ij}c_j=0$ 就可以了. 若 $m<n$，则这个方程组有非平凡解[见第一章(2.17)]，从而 L 线性相关. ■

【3.17】命题 向量空间 V 的两个基 $\boldsymbol{B}_1$，$\boldsymbol{B}_2$ 有相同数量的元素.

证明 在(3.16)中取 $\boldsymbol{B}_1=S$，$\boldsymbol{B}_2=L$ 得到 $|\boldsymbol{B}_1|\geqslant|\boldsymbol{B}_2|$. 由对称性，$|\boldsymbol{B}_2|\geqslant|\boldsymbol{B}_1|$. ■

【3.18】定义 有限维向量空间 V 的**维数**是一个基中向量的个数. 维数将记为 $\dim V$.

【3.19】命题

(a) 如果 S 张成 V，则 $|S|\geqslant\dim V$，并且仅当 S 是基时等式成立.

(b) 若 L 线性无关，则 $|L|\leqslant\dim V$，并且仅当 L 是基时等式成立.

证明 这可由(3.13)和(3.15)得到. ■

【3.20】命题 若 $W\subset V$ 是有限维向量空间的一个子空间. 则 W 是有限维的且 $\dim W\leqslant\dim V$. 此外，$\dim W=\dim V$ 仅当 $W=V$.

证明 只要我们证明了 W 是有限维的，命题就是显然的了．这是因为，如果 $W<V$，即如果 W 属于但不等于 V，则 W 的基将不会张成 V，但由(3.15)它可以扩张成 V 的一个基．因此 $\dim W<\dim V$．我们现在验证维数有限：如果某个给定的 W 中的线性无关子集 L 不能张成 W，则存在向量 $w\in W$ 不属于 $\mathrm{Span}L$，且由命题(3.10)，(L, w)线性无关．这样，我们可以从空集开始，利用(3.10)不断添加 W 的元素而希望最后得到 W 的一个基．显然，如果 L 是 W 的一个线性无关子集，则把它视为 V 的子集仍是线性无关的．从而(3.16)告诉我们 $|L|\leqslant n=\dim V$．这样在 L 上添加元素的过程最多在 n 步后就要终止．当不能再用(3.16)添加元素时，L 就成了 W 的基．这表明 W 是有限维的，正是所要证的． ■

注意

(a) 要记住的关键事实是(3.13)、(3.15)和(3.16)．其余的结论可由它们得到．

(b) 这些内容不深．给出定义，你可以在几天或更少的时间得出主要结论(3.16)的证明，虽然第一次尝试时可能会不太优美．

向量空间的一个重要例子，是从任意集合 S 出发，通过形式地构造系数在 F 中的 S 中元素的线性组合而得到的．若 $S=(s_1, \cdots, s_n)$是元素互不相同的有限有序集，则这个空间 $V=V(S)$是所有表达式

93 **【3.21】**

$$a_1 s_1+\cdots+a_n s_n, a_i\in F$$

的集合．加法和标量乘法都是在假设元素 s_i 间没有关系的前提下形式地进行的：

【3.22】

$$(a_1 s_1+\cdots+a_n s_n)+(b_1 s_1+\cdots+b_n s_n)=(a_1+b_1)s_1+\cdots+(a_n+b_n)s_n$$

$$c(a_1 s_1+\cdots+a_n s_n)=(ca_1)s_1+\cdots+(ca_n)s_n.$$

这个向量空间在对应

【3.23】

$$(a_1,\cdots,a_n)\rightsquigarrow a_1 s_1+\cdots+a_n s_n$$

下同构于 F^n．于是解释为线性组合

$$s_1=1s_1+0s_2+\cdots+0s_n$$

的元素 s_i 构成在同构(3.23)下对应于 F^n 的标准基的一个基．正因为这一点，$V(S)$称为以 S 为基的空间，或 S 的形式线性组合的空间．如果 S 无限，$V(S)$定义为所有有限表达式(3.21)的空间，其中$s_i\in S$(见第五节)．

因为当 S 含有 n 个元素时 $V(S)$同构于 F^n，从逻辑上讲，我们现在并不是非引入它不可．然而在许多运用中，$V(S)$有着自然的解释．例如，如果 S 是配料，那么一个向量 v 代表一个配方．或者，如果 S 是平面上的一个点集，则 v[(3.21)]可解释为在 S 的点上的重量的集合．

第四节 用基计算

向量空间中引入基的目的是提供一种计算的方法，本节我们将学习如何使用它．我们将考虑两个主题：如何用一组给定的基表出一个向量，以及如何将同一个向量空间的两个不同的基联系起来．

设给定向量空间 V 的一个基$(v_1, \cdots, v_n)$．记住：这意味着每个向量 $v\in V$ 可以用恰好一

种形式表示为线性组合

【4.1】
$$v = x_1 v_1 + \cdots + x_n v_n, x_i \in F.$$

标量 x_i 称为 v 的坐标，而列向量

【4.2】
$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

称为 v 关于这个基的坐标向量．我们考虑计算这个坐标向量的问题．

要理解的最简单情形是 V 是列向量空间 F^n．设 $\boldsymbol{B}=(v_1, \cdots, v_n)$ 是 F^n 的一个基．则基中的每个元 v_i 是一个列向量，因而数组$(v_1, \cdots, v_n)$构成一个 $n \times n$ 矩阵．对这个矩阵引入一个新符号似乎是明智的，因而我们将它写作 94

【4.3】
$$[\boldsymbol{B}] = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix}.$$

例如，如果 $\boldsymbol{B}$ 是基

【4.4】
$$v_1 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 3 \\ 5 \end{bmatrix}, \quad 则[\boldsymbol{B}] = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}.$$

若 $\boldsymbol{E}=(e_1, \cdots, e_n)$是标准基，则矩阵$[\boldsymbol{E}]$是单位矩阵．

一个线性组合 $x_1 v_1 + \cdots + x_n v_n$ 可以写为矩阵乘积

【4.5】
$$[\boldsymbol{B}]X = \begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = v_1 x_1 + \cdots + v_n x_n,$$

其中 X 表示列向量$(x_1, \cdots, x_n)^t$．这是分块乘法的另一个例子．其仅有的新特性是根据矩阵乘法的定义，标量系数 x_i 移到了向量的右边，但这是没有关系的．

若给定一个向量 $Y=(y_1, \cdots, y_n)^t$，可以通过对未知向量 X 解方程

【4.6】
$$\begin{bmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \quad 或 \quad [\boldsymbol{B}]X = Y$$

确定它关于基 $\boldsymbol{B}$ 的坐标向量．这可由对矩阵$[\boldsymbol{B}]$取逆做到．

【4.7】命题 *设 $\boldsymbol{B}=(v_1, \cdots, v_n)$是 F^n 的一个基，并设 $Y \in F^n$ 是一个向量．Y 关于基 $\boldsymbol{B}$ 的坐标向量是*

$$X = [\boldsymbol{B}]^{-1} Y.$$

注意，如果 $\boldsymbol{B}$ 是标准基 $\boldsymbol{E}$，我们又得到了 Y，因为$[\boldsymbol{E}]$是单位矩阵．这正是应得到的．

在例(4.4)中，

$$[\boldsymbol{B}]^{-1} = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}^{-1} = \begin{bmatrix} -5 & 3 \\ 2 & -1 \end{bmatrix}.$$

95

因而 $Y=\begin{bmatrix}1\\4\end{bmatrix}$ 的坐标向量是 $X=\begin{bmatrix}7\\-2\end{bmatrix}$，也就是 $Y=7v_1-2v_2$.

当然，除非矩阵可逆，否则是不能这样求解的．幸运的是，$[\boldsymbol{B}]$总是可逆的，事实上它可以是任意的可逆矩阵．

【4.8】命题 设 A 是一个元素属于域 F 的 $n\times n$ 矩阵．A 的列向量构成 F^n 的一个基当且仅当 A 是可逆的．

证明 记 A 的第 i 个列向量为 v_i．对任意列向量 $X=(x_1, \cdots, x_n)^t$，矩阵乘积 $AX=v_1x_1+\cdots+v_nx_n$ 是集$(v_1, \cdots, v_n)$的线性组合．因此，这个集合线性无关当且仅当方程 $AX=0$ 仅有的解是平凡解 $X=0$．如我们所知，这一结论成立当且仅当 A 是可逆的[第一章(2.18)]．而且，如果$(v_1, \cdots, v_n)$是线性无关集，则因为 F^n 的维数是 n，它构成一个基． ■

现在假设 V 是一个抽象给出的向量空间．我们想用矩阵记号简化基的使用，我们在选择写出向量有序集的方式时就已经考虑到了这一点：

【4.9】
$$(v_1,\cdots,v_n).$$

也许这个数组应称为超向量．除非向量都是具体给出的，否则将不能用矩阵代表这个超向量，因此我们将形式地使用它，就好像它是一个向量．因为向量空间中两个元素的乘法没有定义，所以不能将两个元素是向量的矩阵相乘．但可以用标量矩阵去乘超向量$(v_1, \cdots, v_m)$．这样，这些向量的线性组合可写为与列向量 X 的乘积：

【4.10】
$$(v_1,\cdots,v_m)\begin{bmatrix}x_1\\ \vdots\\ x_m\end{bmatrix}=v_1x_1+\cdots+v_mx_m.$$

求这个积的值，就得到另一个向量——它们的一个线性组合．像前面一样，系数 x_i 在向量的右边．如果用形如 $\boldsymbol{B}$ 的记号表示集$(v_1, \cdots, v_m)$，则这个线性组合的记号变得非常紧凑：$\boldsymbol{B}X=v_1x_1+\cdots+v_nx_n$.

我们也可以用标量矩阵从右边去乘一个超向量．如果 A 是一个 $m\times n$ 矩阵，积将是另一个超向量，比如说$(w_1, \cdots, w_n)$：

【4.11】
$$(v_1,\cdots,v_m)\begin{bmatrix} & & \\ & A & \\ & & \end{bmatrix}=(w_1,\cdots,w_n).$$

要对积求值，可以应用矩阵乘法法则：

【4.12】
$$w_j=v_1a_{1j}+v_2a_{2j}+\cdots+v_ma_{mj}.$$

96

因此，每一个向量 w_j 都是$(v_1, \cdots, v_m)$的线性组合，并且这个线性组合的标量系数构成矩阵 A 的列．这正是等式的含义．例如，

$$(v_1,v_2)\begin{bmatrix}3&2&1\\4&0&1\end{bmatrix}=(3v_1+4v_2,2v_1,v_1+v_2).$$

下面正式地复述这一点：

【4.13】命题 设 $S=(v_1, \cdots, v_m)$和 $U=(w_1, \cdots, w_n)$为向量空间 V 中元素的有序集．U 的元素属于 S 的张成当且仅当存在一个 $m\times n$ 标量矩阵 A，使得$(v_1, \cdots, v_m)A=(w_1, \cdots, w_n)$.

现在我们考虑确定给定的向量 $v\in V$ 关于一组给定基 $\boldsymbol{B}=(v_1, \cdots, v_n)$的坐标向量 X 的问

题. 也就是说，我们希望如(4.10)那样具体地写出 $v=\boldsymbol{B}X$. 很显然，除非基和向量都以某种具体的方式给出，否则这是不可能的，因而我们不能解决所提出的问题，但可以用超向量 $\boldsymbol{B}$ 的乘法抽象地定义一个由列向量空间 F^n 到 V 的向量空间的同构

【4.14】

$$\psi: F^n \longrightarrow V \text{使}$$
$$X \rightsquigarrow \boldsymbol{B}X.$$

这个映射是一一映射，这是因为每个向量 v 恰好以一种方式写为线性组合(4.10)——因为集合 $\boldsymbol{B}$ 张成 V，所以它是满射；而因为 $\boldsymbol{B}$ 线性无关，所以它是单射. 容易验证同构的公理(2.13). 我们可以利用这个同构将坐标引入向量空间 V 中.

一个向量 v 的坐标向量是 $X=\psi^{-1}(v)$. 请注意，符号 $\boldsymbol{B}^{-1}$ 没有定义. 因此，除非进一步明确地给出基，否则不会有逆函数 $\psi^{-1}(v)$ 的精确公式. 但同构 ψ 的存在本身就很有意义.

【4.15】推论 每个 n 维向量空间 V 同构于列向量空间 F^n.

注意，如果 $m\neq n$，F^n 与 F^m 不同构，因为 F^n 有具有 n 个向量的基，而基中元素的个数仅依赖于向量空间，而不依赖于基的选择. 这样，域 F 上的有限维向量空间被(4.15)完全分类：对唯一确定的 n，每个 V 同构于 F^n. 由此可得，如果研究列向量空间这一基本例子，我们将知道所有任意的空间. 一旦给定一个基，向量空间的任何问题就化简为熟悉的列向量的代数.

我们现在遇到了一个重要的计算方法：基变换. 当给出一个自然的基时，将 V 与同构的向量空间 F^n 等同起来是有用的，而当给出的基对问题不太合适时，那就不行了. 这种情况下，我们想要改变坐标. 因此，假设对同一个向量空间 V 有两个基，如 $\boldsymbol{B}=(v_1, \cdots, v_n)$ 和 $\boldsymbol{B}'=(v'_1, \cdots, v'_n)$. 将 $\boldsymbol{B}$ 看作旧基而将 $\boldsymbol{B}'$ 看作新基. 有两个计算我们想要搞清楚. 首先问：两个基是如何联系起来的？其次，一个向量 $v\in V$ 关于每一个基都有坐标，它们当然是不同的. 因而我们问：两个坐标向量是如何联系起来的？这些就是称为基变换的计算. 在后面几章中它们将是非常重要的. 它们也易于引起混乱，如果你的记号组织得不好，它们会让你头疼.

首先注意，由于新基张成 V，旧基 $\boldsymbol{B}$ 中的每个向量是新基 $\boldsymbol{B}'=(v'_1, \cdots, v'_n)$ 的一个线性组合. 于是，由命题(4.13)，存在形如

【4.16】

$$(v'_1, \cdots, v'_n)\left[\quad P \quad\right]=(v_1, \cdots, v_n), \quad \text{或 } \boldsymbol{B}'P=\boldsymbol{B}$$

的等式，其中 P 是 $n\times n$ 标量矩阵. 这个矩阵等式给出

【4.17】

$$v'_1 p_{1j}+v'_2 p_{2j}+\cdots+v'_n p_{nj}=v_j,$$

其中 p_{ij} 是 P 的元素. 矩阵 P 称为基变换的矩阵. 其第 j 列是旧基向量 v_j 关于新基 $\boldsymbol{B}'$ 计算出来的坐标向量.

注意基变换的矩阵是可逆的. 这可证明如下：交换 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$ 给出矩阵 P' 使得 $\boldsymbol{B}P'=\boldsymbol{B}'$. 与(4.16)结合起来得到关系 $\boldsymbol{B}P'P=\boldsymbol{B}$：

$$(v_1, \cdots, v_n)\left[\quad P'P \quad\right]=(v_1, \cdots, v_n).$$

这个公式把 v_i 表成 $(v_1, \cdots, v_n)$ 的线性组合. 矩阵乘积 $P'P$ 的元素为其系数. 但因为 $\boldsymbol{B}$ 是线性无关集合，只有一种把 v_i 写成 $(v_1, \cdots, v_n)$ 的线性组合的形式，即 $v_i=v_i$，或 $\boldsymbol{B}I=\boldsymbol{B}$. 于是

97

$P'P=I$. 这就证明了 P 是可逆的.

现在假设 X 是 v 关于旧基 $\boldsymbol{B}$ 计算出来的坐标向量，即 $v=\boldsymbol{B}X$. 代入(4.16)给出矩阵方程

【4.18】 $$v=\boldsymbol{B}X=\boldsymbol{B}'PX.$$

这个方程指出 $PX=X'$ 是 v 关于新基 $\boldsymbol{B}'$ 的坐标向量.

回顾一下，我们有单个矩阵 P——基变换矩阵，它具有对偶的性质：

【4.19】 $$\boldsymbol{B}=\boldsymbol{B}'P \quad 和 \quad PX=X',$$

98

其中 X，X' 表示任意向量 v 关于两个基的坐标向量. 每一个性质都刻画了 P. 仔细注意撇的位置.

当 $V=F^n$ 且旧基为标准基 $\boldsymbol{E}$，而新基 $\boldsymbol{B}'$ 是任意的时，我们可以具体地算出基变换的矩阵. 如(4.3)，两个基确定矩阵$[\boldsymbol{E}]=I$ 和$[\boldsymbol{B}']$. 公式(4.19)给出矩阵方程 $I=[\boldsymbol{B}']P$，因而基变换的矩阵为

【4.20】 $$P=[\boldsymbol{B}']^{-1} \quad 如果 V=F^n 且旧基是 \boldsymbol{E}.$$

这也可记为$[\boldsymbol{B}']=P^{-1}$. 于是有以下结论.

【4.21】 *如果旧基是 $\boldsymbol{E}$，则新基向量是 P^{-1} 的列向量.*

在上面的讨论中，矩阵 P 由两个基 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$ 决定. 我们亦可把讨论转过来，从一个基 $\boldsymbol{B}$ 和一个可逆矩阵 $P\in GL_n(F)$ 开始. 则可由公式(4.16)定义一个新基，即

【4.22】 $$\boldsymbol{B}'=\boldsymbol{B}P^{-1}.$$

因为 $\boldsymbol{B}=\boldsymbol{B}'P$[(4.13)]，所以构成旧基的向量 v_i 都属于 $\boldsymbol{B}'$ 的张成. 因此 $\boldsymbol{B}'$ 张成 V，而且元素个数合适，因而 $\boldsymbol{B}'$ 是基.

【4.23】推论 *设 $\boldsymbol{B}$ 是向量空间 V 的基，则其他基是形如 $\boldsymbol{B}'=\boldsymbol{B}P^{-1}$ 的集合，其中 $P\in GL_n(F)$ 是可逆矩阵.*

当然，在叙述中不一定非要加上逆矩阵. 因为 P 任意，P^{-1} 也任意，我们也可以取 $P^{-1}=Q$ 而说 $\boldsymbol{B}'=\boldsymbol{B}Q$，其中 $Q\in GL_n(F)$.

作为上述讨论的一个应用，我们计算当 $F=\mathbb{F}_p$ 时一般线性群 $GL_2(F)$ 的阶. 通过计算向量空间 $V=F^2$ 的维数来进行. 因为 V 的维数是 2，任何两个元素的线性无关集合(v_1, v_2)构成一个基. 线性无关集合的第一个元素 v_1 是非零的. 且由于 F 的阶为 p，包括 0，V 中有 p^2 个元素. 因而对于向量 v_1 有 p^2-1 种选择. 其次，当 v_1 不为零时，两个向量的集合(v_1, v_2)线性无关当且仅当 v_2 不是 v_1 的倍数[(3.7)]. 给定向量 v_1 的倍元共有 p 个. 因而，当 v_1 给定时，共有 p^2-p 个向量 v_2 使(v_1, v_2)线性无关. 这总共给出

$$(p^2-1)(p^2-p)=p(p+1)(p-1)^2$$

个 V 的基.

【4.24】推论 *一般线性群 $GL_2(\mathbb{F}_p)$ 的阶为 $p(p+1)(p-1)^2$.*

99

证明 命题(4.23)建立了 F^n 的基与 $GL_n(F)$ 的元素间的一一对应. ■

第五节 无限维空间

有的向量空间太大了，无法由任意有限的向量集合张成. 它们被称为是*无限维的*. 我们并不常用到它们，但因为它们在分析中很重要，所以本节将对它们稍作讨论.

无限维向量空间最明显的例子是无限实向量

【5.1】
$$(a)=(a_1,a_2,a_3,\cdots)$$
的空间$\mathbb{R}^\infty$. 也可以把它看作是实数序列$\{a_n\}$的空间. 例(1.8c、d)也是无限维的.

空间$\mathbb{R}^\infty$有许多重要的子空间，下面是一些例子.

【5.2】例

(a) 收敛序列：$C=\{(a)\in\mathbb{R}^\infty \mid \lim\limits_{n\to\infty} a_n$ 存在$\}$.

(b) 有界序列：$\ell^\infty=\{(a)\in\mathbb{R}^\infty \mid \{a_n\}$有界$\}$.

序列$\{a_n\}$是有界的，如果存在某个实数 b，也就是它的界，使得对所有 n，$|a_n|\leqslant b$ 成立.

(c) 绝对收敛级数：$\ell^1=\left\{(a)\in\mathbb{R}^\infty \mid \sum\limits_1^\infty |a_n|<\infty\right\}$.

(d) 有限项非零的序列：

$$Z=\{(a)\in\mathbb{R}^\infty \mid a_n=0 \text{ 对除有限多个以外的 } n \text{ 成立}\}.$$

所有上面的空间都是无限维的. 还可以找出更多的无限维空间.

现在设 V 是向量空间，是否无限维都行. 向量的无限集 S 的张成应该是什么呢？困难在于：不可能以一致的方式找到一个向量，作为无限多个向量的线性组合 $c_1v_1+c_2v_2+\cdots$ 的取值. 如果讨论的是实数的向量空间，即 $v_i\in\mathbb{R}^1$，假如级数 $c_1v_1+c_2v_2+\cdots$收敛，则可以为它指定一个值. 对于$\mathbb{R}^n$ 或$\mathbb{R}^\infty$ 中的收敛级数，同样可以这样做. 但许多级数不收敛，我们就不知道该指定什么值了.

在代数中，习惯上只谈论有限多个向量的线性组合. 因此，无限集 S 的张成必须解释为由那些是 S 中有限多个元素的线性组合的向量 v 组成的集合：

【5.3】
$$v=c_1v_1+\cdots+c_rv_r,\quad \text{其中 } v_1,\cdots,v_r\in S.$$
数 r 可以任意大，与向量 v 有关：

【5.4】
$$\mathrm{Span}S=\{S\text{ 中元素的有限线性组合}\}.$$
有了这个定义，命题(3.2)和(3.11)仍然成立.

100

例如，设 $e_i=(0,\ \cdots,\ 0,\ 1,\ 0,\ \cdots)$是$\mathbb{R}^\infty$中第 i 个位置值为 1 且是它仅有的非零坐标的向量. 设 $S=(e_1,\ e_2,\ e_3,\ \cdots)$是这些向量 e_i 的无限集合. 集合 S 不能张成$\mathbb{R}^\infty$，因为向量
$$w=(1,1,1,\cdots)$$
不是一个(有限)线性组合. 而由 S 的张成是子空间 Z(5.2d).

一个集合 S，不论是否无限，称为线性无关的，如果除了在下式中使 $c_1=\cdots=c_r=0$ 的平凡关系外，没有其他的有限关系：

【5.5】
$$c_1v_1+\cdots+c_rv_r=0,\quad v_1,\cdots,v_r\in S.$$
这里数 r 也允许是任意的，即条件对任意大的 r 及任意向量 $v_1,\ \cdots,\ v_r\in S$ 都成立. 例如，假如 w，e_i 是前面定义的向量，集合 $S'=(w;\ e_1,\ e_2,\ e_3,\ \cdots)$是线性无关的. 在这个线性无关的定义下，命题(3.10)仍旧成立.

与有限集一样，V 的基 S 是张成 V 的一个线性无关集合. 这样 $S=(e_1,\ e_2,\ e_3,\ \cdots)$是空间 Z 的基. 应用选择公理可以证明每个向量空间都有一个基. 然而，证明中并没有指出如何得到一个基. $\mathbb{R}^\infty$的一个基中将有多达不可数的元素，因而它无法被明确地写出. 对无限维空间，

我们不常需要基.

暂时回到向量空间是有限维的情形(3.12)，问是否会存在一个无限基. 在第三节，我们看到任意两个有限基都有同样多的元素. 我们现在证明每个基都是有限的，从而完成讨论. 唯一混乱的地方由下面的命题来处理.

【5.6】命题 设 V 是有限维的，并设 S 是张成 V 的任意集合. 则 S 中含有一个张成 V 的有限子集.

证明 由假设，有一个有限集$(w_1, \cdots, w_m)$，它张成空间 V. 因为 $\operatorname{Span}S=V$，所以每一个 w_i 是 S 中有限多个元素的线性组合. 因而当将向量 $w_1, \cdots, w_m$ 用集合 S 表出时，我们仅需要其中的有限多个元素. 我们用到的元素组成一个有限子集 $S'\subset S$. 于是$(w_1, \cdots, w_m)\subset \operatorname{Span}S'$. 因为$(w_1, \cdots, w_m)$张成 V，S'亦张成 V. ■

【5.7】命题 设 V 是有限维向量空间.

(a) 每个张成 V 的集合 S 含有一个有限基.

(b) 每个线性无关集 L 是有限的，因而扩张为一个有限基.

(c) 每个基都是有限的.

101 我们将证明留作练习.

第六节 直 和

设 V 是向量空间，并设 $W_1, \cdots, W_n$ 是 V 的子空间. 关于线性无关和向量张成的大部分做法对于子空间都是类似的，本节将讨论这些类似性质.

考虑向量 $v\in V$，它可以写为和

【6.1】
$$v=w_1+\cdots+w_n,$$

其中 w_i 是 W_i 的向量. 所有这样向量的集合称为子空间的和或它们的张成，记为

【6.2】
$$W_1+\cdots+W_n=\{v\in V \mid v=w_1+\cdots+w_n,\quad \text{其中 } w_i\in W_i\}.$$

类似于向量集合$(v_1, \cdots, v_n)$的张成，和也是 V 的子空间. 很显然，它是含有 $W_1, \cdots, W_n$ 的最小子空间.

子空间 $W_1, \cdots, W_n$ 称为无关的，如果除了对所有 i，$w_i=0$ 的平凡和外，其余的和 $w_1+\cdots+w_n$(其中 $w_i\in W_i$)皆不为零. 换言之，空间是无关的，如果

【6.3】
$$w_1+\cdots+w_n=0 \quad \text{并且} \quad w_i\in W_i \text{ 蕴涵着对所有 } i, w_i=0.$$

在张成是整个空间而且子空间无关时，我们称 V 是 $W_1, \cdots, W_n$ 的直和，并记为

【6.4】
$$V=W_1\oplus\cdots\oplus W_n, \text{如果 } V=W_1+\cdots+W_n \text{ 并且 } W_1,\cdots,W_n \text{ 是无关的.}$$

这是指，每个向量 $v\in V$ 恰好可以以一种方式写为(6.1)的形式.

于是，如果 $W_1, \cdots, W_n$ 是一个向量空间 V 的无关子空间，且 $U=W_1+\cdots+W_n$ 是它们的和，则事实上 $U=W_1\oplus\cdots\oplus W_n$ 是它们的直和.

我们将下列两个命题的证明留作练习.

【6.5】命题

(a) 单个子空间 W_1 是无关的.

(b) 两个子空间 W_1，W_2 无关当且仅当 $W_1\cap W_2=(0)$.

【6.6】命题 设 $W_1, \cdots, W_n$ 是有限维向量空间 V 的子空间，且设 $\boldsymbol{B}_i$ 是 W_i 的基.

(a) 将基 $\boldsymbol{B}_1$，…，$\boldsymbol{B}_n$ 按顺序排起来得到的有序集 $\boldsymbol{B}$ 是 V 的基当且仅当 V 是直和 $W_1\oplus\cdots\oplus W_n$.

(b) $\dim(W_1+\cdots+W_n)\leqslant(\dim W_1)+\cdots+(\dim W_n)$，其中等式成立当且仅当空间是无关的. [102]

【6.7】推论 设 W 是有限维向量空间 V 的子空间. 存在另一个子空间 W'，使 $V=W\oplus W'$.

证明 设$(w_1, \cdots, w_d)$是 W 的基. 扩张为 V 的一个基$(w_1, \cdots, w_d; v_1, \cdots, v_{n-d})$ [(3.15)]. $(v_1, \cdots, v_{n-d})$的张成即为所求的子空间 W'. ■

【6.8】例 设 v_1，…，v_n 是非零向量，并设 W_i 是单个向量 v_i 的张成. 这是由 v_i 的标量倍所组成的一维子空间：$W_i=\{cv_i\}$. 则 W_1，…，W_n 是无关子空间当且仅当$(v_1, \cdots, v_n)$是线性无关向量. 如果比较(3.4)和(6.3)就很清楚了. 用子空间的叙述更为整洁，因为标量系数都被去掉了.

【6.9】命题 设 W_1，W_2 是一个有限维向量空间 V 的子空间. 则

$$\dim W_1+\dim W_2=\dim(W_1\cap W_2)+\dim(W_1+W_2).$$

证明 注意两个子空间之交仍是子空间. 选择 $W_1\cap W_2$ 的一个基$(u_1, \cdots, u_r)$，其中 $r=\dim(W_1\cap W_2)$. 这是一个线性无关集，且属于 W_1. 因而，可以把它扩张为 W_1 的一个基，比如说

【6.10】 $$(u_1,\cdots,u_r;x_1,\cdots,x_{m-r}),$$

其中 $m=\dim W_1$. 类似地，可将它扩张为 W_2 的一个基

【6.11】 $$(u_1,\cdots,u_r;y_1,\cdots,y_{n-r}),$$

其中 $n=\dim W_2$. 如果证明集合

【6.12】 $$(u_1,\cdots,u_r;x_1,\cdots,x_{m-r};y_1,\cdots,y_{n-r})$$

是 W_1+W_2 的基，则得到命题.

这个断言有两部分. 首先，(6.12)的向量张成 W_1+W_2. 因为任意 W_1+W_2 的向量是一个和 $v=w_1+w_2$，而 $w_i\in W_i$. 可以把 w_1 写成(6.10)的线性组合，而把 w_2 写成(6.11)的线性组合. 合并相同的项，得到 v 是(6.12)的线性组合.

其次，(6.12)的向量线性无关：设某个线性组合为零，比如说

$$a_1u_1+\cdots+a_ru_r+b_1x_1+\cdots+b_{m-r}x_{m-r}+c_1y_1+\cdots+c_{n-r}y_{n-r}=0.$$

简记为 $u+x+y=0$. 解出 y 得：$y=-u-x\in W_1$. 但也有 $y\in W_2$. 于是 $y\in W_1\cap W_2$，从而 y 是$(u_1, \cdots, u_r)$的线性组合，记为 u'. 则 $-u'+y=0$ 是(6.11)向量间的关系，而这些向量线性无关. 因而，它必为平凡关系. 这证明了 $y=0$. 从而，原来的关系化为 $u+x=0$. 因为(6.10)是基，这个关系是平凡的：$u=0$ 且 $x=0$. 因而整个关系也是平凡的，正是所需证的. ■ [103]

我不必学 8+7：我将记住 8+8 然后减去 1.

T. Cuyler Young, Jr.

练　习

第一节　实向量空间

1. 实 $n\times n$ 矩阵的下列子集中哪些是子空间？

(a) 对称矩阵($A=A^t$)

(b) 可逆矩阵

(c) 上三角矩阵

2. 证明两个子空间的交是子空间.
3. 证明向量空间中的消去律：若 $cv=cw$ 且 $c\neq 0$，则 $v=w$.
4. 证明：若 w 是子空间 W 的一个元素，则也有 $-w\in W$.
5. 证明在(1.2)后叙述的$\mathbb{R}^3$ 的子空间的分类是完全的.
6. 证明方程 $2x_1-x_2-2x_3=0$ 的每个解具有(1.5)的形式.
7. 由特解 $u_1=(2, 2, 1)$及 $u_2=(0, 2, -1)$得到的类似(1.4)的描述是什么？

第二节　抽象域

1. 证明形如 $a+b\sqrt{2}$的数的集合是一个域，其中 a，b 是有理数.
2. $\mathbb{C}$ 的哪个子集关于+，-，×和÷都闭但不含 1？
3. 设 F 是$\mathbb{C}$ 的子集，使得 F^+ 是$\mathbb{C}^+$ 的子群而 $F^\times$ 是$\mathbb{C}^\times$ 的子群. 证明 F 是$\mathbb{C}$ 的子域.
4. 设 $V=F^n$ 是列向量空间. 证明 V 的每个子空间 W 是某个齐次线性方程组 $AX=0$ 的解空间.
5. 证明一个向量空间的非空子集 W 满足子空间的条件(2.12)当且仅当它在加法和标量乘法下封闭.
6. 证明在定义(2.3)中，公理(ii)可用下面的公理代替：$F^\times$ 是阿贝尔群且 $1\neq 0$. 如果去掉 $1\neq 0$ 的条件会怎样？
7. 定义域的同态，并证明域的每个同态是单射.
8. 对 $p=2, 3, 7, 11, 13$，求 5(模 p)的逆.
9. 当系数视为(a)域$\mathbb{F}_5$ 和(b)域$\mathbb{F}_7$ 中的元素时，计算多项式$(x^2+3x+1)(x^3+4x^2+2x+2)$.
10. 考虑线性方程组$\begin{bmatrix}8 & 3\\ 2 & 6\end{bmatrix}\begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}3\\ -1\end{bmatrix}$.

    (a) 当 $p=5, 11, 17$ 时，在$\mathbb{F}_p$ 中求解.

    104

    (b) 当 $p=7$ 时，求解的个数.
11. 求素数 p 使矩阵
$$A=\begin{bmatrix}1 & 2 & 0\\ 0 & 3 & -1\\ -2 & 0 & 2\end{bmatrix}$$
    当其元在$\mathbb{F}_p$ 中时可逆.
12. 完全地解线性方程组 $AX=B$，其中
$$A=\begin{bmatrix}1 & 1 & 0\\ 1 & 0 & 1\\ 1 & -1 & -1\end{bmatrix},\quad B=\begin{bmatrix}0\\ 0\\ 0\end{bmatrix}\quad 和\quad B=\begin{bmatrix}1\\ -1\\ 1\end{bmatrix}$$
    (a)在$\mathbb{Q}$ 中，(b)在$\mathbb{F}_2$ 中，(c)在$\mathbb{F}_3$ 中，(d)在$\mathbb{F}_7$ 中.
13. 设 p 是素整数，$\mathbb{F}_p$ 的非零元素构成一个阶为 $p-1$ 的群$\mathbb{F}_p^\times$. 事实上，这个群总是一个循环群. 对所有素数$p<20$ 通过找出其生成元验证.
14. (a) 设 p 是素数，利用$\mathbb{F}_p^\times$ 是群这一事实证明对每个不同余于零的整数 a 有 $a^{p-1}\equiv 1$(模 p).

    (b) 证明费马定理：对每个整数 a，
$$a^p\equiv a(模\ p).$$
15. (a) 通过元素与其逆元素的配对证明$\mathbb{F}_p$ 的所有非零元素的乘积为-1.

    (b) 设 p 是素数，证明威尔逊定理：

$$(p-1)!\equiv -1(\text{模 } p).$$

16. 考虑有 n 个未知量的 n 个线性方程的线性方程组 $AX=B$，其中 A 和 B 都有整元素. 证明或反证：若方程组有整数解，则它对所有 p 在 $\mathbb{F}_p$ 中有解.

17. 在域 $\mathbb{F}_2$ 中解释矩阵元素，证明四个矩阵 $\begin{bmatrix}1&0\\0&1\end{bmatrix}$，$\begin{bmatrix}0&0\\0&0\end{bmatrix}$，$\begin{bmatrix}1&1\\1&0\end{bmatrix}$，$\begin{bmatrix}0&1\\1&1\end{bmatrix}$ 构成一个域.

18. 引理(2.8)的证明中含有(2.6)的一个更直接的证明. 把它抽取出来.

第三节　基和维数

1. 求 $\mathbb{R}^4$ 中由向量(1, 2, −1, 0), (4, 8, −4, −3), (0, 1, 3, 4), (2, 5, 1, 4)张成的子空间的基.
2. 设 $W\subset\mathbb{R}^4$ 是线性方程组 $AX=0$ 的解空间，其中 $A=\begin{bmatrix}2&1&2&3\\1&1&3&0\end{bmatrix}$. 求 W 的基.
3. (a) 证明线性无关集合的子集线性无关.
   (b) 证明基的任意重排序仍是基.
4. 设 V 是 F 上的 n 维向量空间，并设 $0\leqslant r\leqslant n$. 证明 V 含有一个 r 维子空间.
5. 求对称 $n\times n$ 矩阵空间的一个基.
6. 证明方阵 A 可逆当且仅当其列向量线性无关.
7. 设 V 是区间[0, 1]上的函数向量空间. 证明函数 x^3，$\sin x$ 和 $\cos x$ 是线性无关的.
8. 设 A 是一个 $m\times n$ 矩阵，并设 A' 为由 A 上作一序列初等行变换得到的矩阵. 证明 A 的行与 A' 的行张成同样的子空间.
9. 设 V 是 n 维复向量空间. 证明作为实向量空间，V 是 $2n$ 维的.
10. 复 $n\times n$ 矩阵称为埃尔米特矩阵，如果对所有 i，j，$a_{ij}=\bar{a}_{ji}$. 证明埃尔米特矩阵构成实向量空间，求空间的基并确定其维数.
11. 向量空间 $\mathbb{F}_p{}^n$ 中有多少元素？
12. 设 $F=\mathbb{F}_2$. 求 F^2 的所有基.
13. 设 $F=\mathbb{F}_5$. 空间 F^3 中每个维数的子空间有多少个？
14. (a) 设 V 是域 $\mathbb{F}_q$ 上的 3 维向量空间. V 中每个维数的子空间有多少个？
    (b) 对 4 维向量空间回答同样的问题.
15. (a) 设 $F=\mathbb{F}_2$. 证明群 $GL_2(F)$ 同构于对称群 S_3.
    (b) 设 $F=\mathbb{F}_3$. 确定 $GL_2(F)$ 和 $SL_2(F)$ 的阶.
16. 设 W 是 V 的子空间.
    (a) 证明存在 V 的子空间 U，使 $U+W=V$ 且 $U\cap W=0$.
    (b) 证明不存在子空间 U，使 $W\cap U=0$ 且 $\dim W+\dim U>\dim V$.

第四节　用基计算

1. 计算 F^2 中将标准基 $\boldsymbol{E}$ 联系到基 $\boldsymbol{B}'=(v_1, v_2)$ 的基变换的矩阵 P，其中 $v_1=(1, 3)^t$，$v_2=(2, 2)^t$.
2. 当旧基是标准基 $(e_1, \cdots, e_n)$ 且新基是 $(e_n, e_{n-1}, \cdots, e_1)$ 时，求基变换的矩阵.
3. 当旧基是标准基 (e_1, e_2) 且新基是 (e_1+e_2, e_1-e_2) 时，求基变换的矩阵.
4. 考虑 $\mathbb{R}^2$ 的等边坐标系，由基 $\boldsymbol{B}'$ 给出，其中 $v_1=e_1$，而 v_2 是与 v_1 夹角为 120°的单位向量. 求将标准基 $\boldsymbol{E}$ 联系到基 $\boldsymbol{B}'$ 的基变换的矩阵.
5. (a) 证明集合 $\boldsymbol{B}=((1, 2, 0)^t, (2, 1, 2)^t, (3, 1, 1)^t)$ 是 $\mathbb{R}^3$ 的基.
   (b) 求向量 $v=(1, 2, 3)^t$ 关于这个基的坐标向量.
   (c) 设 $\boldsymbol{B}'=((0, 1, 0)^t, (1, 0, 1)^t, (2, 1, 0)^t)$. 求将 $\boldsymbol{B}$ 联系到 $\boldsymbol{B}'$ 的矩阵 P.

(d)对哪些素数 p，$\boldsymbol{B}$ 是 $\mathbb{F}_p^3$ 的基？

6. 设 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$ 是向量空间 F^n 的两个基，证明基变换的矩阵为 $P=[\boldsymbol{B}']^{-1}[\boldsymbol{B}]$.

106

7. 设 $\boldsymbol{B}=(v_1,\cdots,v_n)$ 是向量空间 V 的基．证明可以由 $\boldsymbol{B}$ 经过有限步下列类型的作用得到任意一个其他基 $\boldsymbol{B}'$.

   (i) 对某个 $a\in F$，用 v_i+av_j 代替 v_i，$i\neq j$.

   (ii) 对某个 $c\neq 0$，用 cv_i 代替 v_i.

   (iii) 交换 v_i 和 v_j.

8. 用命题(4.13)的记号重写命题(3.16)的证明.

9. 设 $V=F^n$．建立 V 的基的集合 $\mathcal{B}$ 与 $GL_n(F)$ 之间的一一对应.

10. 设 F 是有 81 个元的域，V 是 F 上的 3 维向量空间．求 V 的一维子空间的个数.

11. 设 $F=\mathbb{F}_p$.

    (a) 计算 $SL_2(F)$ 的阶.

    (b) 计算 F^n 的基的个数，以及 $GL_n(F)$ 和 $SL_n(F)$ 的阶.

12. (a) 设 A 是一个 $m\times n$ 矩阵且 $m<n$．通过与在底部加上 $(n-m)$ 行零得到的 $n\times n$ 方阵进行比较，证明 A 没有左逆.

    (b) 设 $\boldsymbol{B}=(v_1,\cdots,v_m)$ 和 $\boldsymbol{B}'=(v'_1,\cdots,v'_n)$ 是向量空间 V 的两个基．通过定义基变换的矩阵并证明其可逆来证明 $m=n$.

第五节　无限维空间

1. 证明书中引入的集合 $(w;e_1,e_2,\cdots)$ 线性无关并描述其张成.

2. 我们也可考虑双边无穷序列 $(a)=(\cdots,a_{-1},a_0,a_1,\cdots)$ 的空间，其中 $a_i\in\mathbb{R}$．证明该空间同构于 $\mathbb{R}^\infty$.

3. 证明空间 Z 同构于实多项式空间.

4. 描述空间 $\mathbb{R}^\infty$ 的另外五个无限维子空间.

5. 对每个正整数 p，可定义空间 ℓ^p 为使得 $\sum|a_i|^p<\infty$ 的序列的空间.

   (a) 证明 ℓ^p 是 $\mathbb{R}^\infty$ 的子空间.

   (b) 证明 $\ell^p<\ell^{p+1}$.

6. 设 V 是由可数无限集张成的向量空间．证明 V 的每个线性无关子集有限或可数无限.

7. 证明命题(5.7).

第六节　直和

1. 证明实 $n\times n$ 矩阵空间 $\mathbb{R}^{n\times n}$ 是对称矩阵 $(A=A^t)$ 空间和反对称矩阵 $(A=-A^t)$ 空间的直和.

2. 设 W 是迹为零的 $n\times n$ 矩阵空间．求子空间 W' 使 $\mathbb{R}^{n\times n}=W\oplus W'$.

3. 证明子空间的和是子空间.

4. 证明命题(6.5).

107

5. 证明命题(6.6).

杂题

1. (a) 证明符号 $\{a+bi\mid a,b\in\mathbb{F}_3\}$ 构成一个九元域，合成法则模仿复数的加法和乘法做出.

   (b) 同样的方法对 $\mathbb{F}_5$ 和 $\mathbb{F}_7$ 是否适合？并解释.

*2. 设 V 是无限域 F 上的向量空间．证明 V 不是其有限多个真子空间的并.

*3. 设 W_1，W_2 是向量空间 V 的子空间．公式 $\dim(W_1+W_2)=\dim W_1+\dim W_2-\dim(W_1\cap W_2)$ 类似于对集合成立的公式 $|S_1\cup S_2|=|S_1|+|S_2|-|S_1\cap S_2|$．如果给出三个集，则有公式

$$|S_1\cup S_2\cup S_3|=|S_1|+|S_2|+|S_3|-|S_1\cap S_2|-|S_1\cap S_3|-|S_2\cap S_3|+|S_1\cap S_2\cap S_3|.$$

对应的子空间的维数公式是否成立？

4. 设 F 是特征不等于 2 的域，且设 $x^2+bx+c=0$ 是系数属于 F 的二次方程. 假定判别式 b^2-4c 是 F 中的一个平方元素，即存在一个元素 $\delta\in F$ 使 $\delta^2=b^2-4c$. 证明二次公式 $x=\frac{(-b+\delta)}{2b}$ 是二次方程在 F 中的解，并且当判别式不是平方时，多项式在 F 中没有根.

5. (a) 元素 $\begin{bmatrix}1 & 1\\ & 1\end{bmatrix}$，$\begin{bmatrix}2 & \\ & 1\end{bmatrix}$ 在 $GL_2(\mathbb{R})$ 中的阶是什么？
   (b) 将矩阵的元素解释为 $\mathbb{F}_7$ 的元素，计算它们在 $GL_2(\mathbb{F}_7)$ 中的阶.

6. 考虑函数 $\det: F^{n\times n}\longrightarrow F$，其中 $F=\mathbb{F}_p$ 是 p 个元素的有限域而 $F^{n\times n}$ 是 $n\times n$ 矩阵集合.
   (a) 证明这个映射是满射.
   (b) 证明所有非零行列式的值取同样多的次数.

7. 设 A 是 $n\times n$ 实矩阵. 证明存在多项式 $f(t)=a_rt^r+a_{r-1}t^{r-1}+\cdots+a_1t+a_0$，它以 A 为根，即有 $a_rA^r+a_{r-1}A^{r-1}+\cdots+a_1A+a_0I=0$. 通过指出矩阵 I，A，A^2，…线性相关证明这个结论.

*8. $\mathbb{R}^2$ 的**代数曲线**是两个变量的多项式 $f(x, y)$ 的零点的轨迹. $\mathbb{R}^2$ 的**多项式路径**是指参数路径 $x=x(t)$，$y=y(t)$，其中 $x(t)$，$y(t)$ 是关于 t 的多项式.
   (a) 通过指出对充分大的 n，函数 $x(t)^iy(t)^j(0\leqslant i, j\leqslant n)$ 线性相关，证明每一多项式路径位于某代数曲线之上.
   (b) 具体求出路径 $x=t^2+t$，$y=t^3$ 的象的代数曲线，并将其画出来.

108

第四章 线性变换

思维混乱和推理错误仍笼罩着代数的开端，
这是冷静深思的人们的诚挚而公正的抱怨.

William Rowan Hamilton 爵士

第一节 维数公式

向量空间中与群同态类似的概念是从域 F 上的一个向量空间到另一个向量空间的映射

$$T:V\longrightarrow W,$$

它与加法和标量乘法相容：

【1.1】
$$T(v_1+v_2)=T(v_1)+T(v_2),\quad T(cv)=cT(v)$$

对所有 V 中的 v_1，v_2 及所有 $c\in F$ 成立. 习惯上把这样的映射叫做线性变换而不是同态. 然而，称为同态也是正确的. 注意一个线性变换与线性组合是相容的：

【1.2】
$$T\left(\sum_i c_iv_i\right)=\sum_i c_iT(v_i).$$

这可由(1.1)通过归纳得到. 注意(1.1)的第一个条件指出 T 是加法群的同态 $V^+\longrightarrow W^+$.

我们已经知道一个线性变换的重要例子，事实上，它是主要的例子：矩阵的左乘. 设 A 为一个元素属于 F 的 $m\times n$ 矩阵，并考虑 A 作为列向量的算子. 它定义一个线性变换

【1.3】
$$F^n\xrightarrow{A左乘}F^m$$
$$X\rightsquigarrow AX.$$

事实上，$A(X_1+X_2)=AX_1+AX_2$，且 $A(cX)=cAX$.

另一个例子：设 P_n 为次数$\leqslant n$ 的形如

【1.4】
$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

的实多项式函数的向量空间. 导数$\frac{\mathrm{d}}{\mathrm{d}x}$是从 P_n 到 P_{n-1}的一个线性变换.

设 T：$V\longrightarrow W$ 是任一线性变换. 类似群同态的情形(第二章第四节)，我们引入两个子空间

【1.5】
$$\ker T=T\text{ 的核}=\{v\in V\mid T(v)=0\},$$
$$\mathrm{im}T=T\text{ 的象}=\{w\in W\mid 对某个\ v\in V, w=T(v)\}.$$

读者可能已经猜到，$\ker T$ 是 V 的子空间，而 $\mathrm{im}T$ 是 W 的子空间.

在 T 为用 A 左乘的情形，对核与象做出解释是有意义的. 在这种情形下，T 的核是齐次线性方程组 $AX=0$ 的解集. T 的象是使得线性方程组 $AX=B$ 有解的向量 $B\in F^m$ 的集合.

本节的主要结果是下面定理中给出的维数公式.

【1.6】定理 设 T：$V\longrightarrow W$ 是一个线性变换，并假定 V 是有限维的. 则

$$\dim V=\dim(\ker T)+\dim(\mathrm{im}T).$$

$\mathrm{im}T$ 和 $\ker T$ 的维数分别称为 T 的秩和零化度. 这样(1.6)可记作

【1.7】 $$\dim V = \text{秩} + \text{零化度}.$$

注意这个公式与群同态公式 $G=|\ker\varphi|\,|\text{im}\varphi|$ 的相似性[第二章(6.15)].

一个 $m\times n$ 矩阵 A 的秩和零化度定义为用 A 左乘的象与核的维数. 我们用 r 表示秩, 用 k 表示零化度. 则 k 是方程 $AX=0$ 的解空间的维数. 使线性方程 $AX=B$ 有解的向量 B 构成象, 这是一个维数为 r 的子空间. 这两个维数的和为 n.

设 B 是用 A 左乘的象中的一个向量, 所以方程 $AX=B$ 至少有一个解 $X=X_0$. 用 K 表示齐次方程 $AX=0$ 的解空间, 即用 A 左乘的核. 则 $AX=B$ 的解集是加法陪集 X_0+K. 这重新叙述了一个熟知的事实: 齐次方程 $AX=0$ 的任意解加上非齐次方程 $AX=B$ 的一个特解, 就得到非齐次方程的另一个解.

设 A 是 $n\times n$ 矩阵. 如果 $\det A\neq 0$, 则如我们所知, 因为 A 可逆, 对每个 B, 方程组 $AX=B$ 有唯一解. 这时 $k=0$ 而 $r=n$. 另一方面, 若 $\det A=0$, 则空间 K 的维数 $k>0$. 由维数公式得到 $r<n$, 这意味着象不是整个空间 F^n. 由此可得, 不是所有方程 $AX=B$ 都有解. 但因为 $AX=B$ 的解集是 K 的陪集, 所以有解的方程一定有多于一个解. [110]

定理(1.6)的证明 假定 $\dim V=n$. 设 $(u_1, \cdots, u_k)$ 是子空间 $\ker T$ 的基, 将它扩张为 V 的一个基[第三章(3.15)]:

【1.8】 $$(u_1,\cdots,u_k;v_1,\cdots,v_{n-k}).$$

对 $i=1, \cdots, n-k$, 令 $w_i=T(v_i)$. 如果证明 $(w_1, \cdots, w_{n-k})=S$ 是 $\text{im}T$ 的基, 则由此可得 $\text{im}T$ 的维数为 $n-k$. 这样将证明定理.

我们需证 S 张成 $\text{im}T$ 且它是一个线性无关集. 设 $w\in\text{im}T$ 为任意元素. 则对 $v\in V$ 有 $w=T(v)$. 用基(1.8)写出 v:

$$v = a_1u_1+\cdots+a_ku_k+b_1v_1+\cdots+b_{n-k}v_{n-k},$$

应用 T, 注意到 $T(u_i)=0$:

$$w = 0+\cdots+0+b_1w_1+\cdots+b_{n-k}w_{n-k}.$$

这样 w 属于 S 张成的空间, 从而 S 张成 $\text{im}T$.

下面假设给定线性关系

【1.9】 $$c_1w_1+\cdots+c_{n-k}w_{n-k}=0,$$

考虑线性组合 $v=c_1v_1+\cdots+c_{n-k}v_{n-k}$, 其中 v_i 是基(1.8)中的向量. 对 v 应用 T 得

$$T(v) = c_1w_1+\cdots+c_{n-k}w_{n-k}=0.$$

这样 $v\in\ker T$. 于是, 可用 $\ker T$ 的基 $(u_1, \cdots, u_k)$ 表出 v, 比如说 $v=a_1u_1+\cdots+a_ku_k$. 则有

$$-a_1u_1-\cdots-a_ku_k+c_1v_1+\cdots+c_{n-k}v_{n-k}=0.$$

但(1.8)是基. 于是 $-a_1=0, \cdots, -a_k=0$ 且 $c_1=0, \cdots, c_{n-k}=0$. 因此关系(1.9)是平凡的. 这表明 S 是线性无关集, 从而完成证明. ■

第二节 线性变换的矩阵

不难证明每一线性变换 $T: F^n \longrightarrow F^m$ 是用一个 $m\times n$ 矩阵 A 左乘. 为此, 考虑 F^n 的标准基向量 e_j 的象 $T(e_j)$. 我们如下标记这些向量的元素:

【2.1】 $$T(e_j)=\begin{bmatrix}a_{1j}\\ \vdots\\ a_{mj}\end{bmatrix},$$

111

构造以这些向量为列向量的 $m\times n$ 矩阵 $A=(a_{ij})$. 将标量写在右边，可将 F^n 的任意向量 $X=(x_1,\cdots,x_n)^t$ 写为 $X=e_1x_1+\cdots+e_nx_n$ 的形式. 则有

$$T(X)=\sum_j T(e_j)x_j=\begin{bmatrix}a_{11}\\ \vdots\\ a_{m1}\end{bmatrix}x_1+\cdots+\begin{bmatrix}a_{1n}\\ \vdots\\ a_{mn}\end{bmatrix}x_n=AX.$$

例如，使得

$$T(e_1)=\begin{bmatrix}1\\2\end{bmatrix}\quad 及\quad T(e_2)=\begin{bmatrix}-1\\0\end{bmatrix}$$

的线性变换 $T:\mathbb{R}^2\longrightarrow\mathbb{R}^2$ 是用矩阵

$$A=\begin{bmatrix}1&-1\\2&0\end{bmatrix}$$

左乘. 若 $X=\begin{bmatrix}x_1\\x_2\end{bmatrix}=e_1x_1+e_2x_2$，则

$$T(X)=\begin{bmatrix}1\\2\end{bmatrix}x_1+\begin{bmatrix}-1\\0\end{bmatrix}x_2=\begin{bmatrix}1&-1\\2&0\end{bmatrix}\begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1-x_2\\2x_1\end{bmatrix}.$$

使用第三章第四节建立的记号，一旦给定两个空间的基，就可以对任意线性变换 $T:V\longrightarrow W$ 作类似的计算. 设 $\boldsymbol{B}=(v_1,\cdots,v_n)$ 和 $\boldsymbol{C}=(w_1,\cdots,w_m)$ 分别为 V 和 W 的基，用简短记号 $T(\boldsymbol{B})$ 表示超向量

$$T(\boldsymbol{B})=(T(v_1),\cdots,T(v_n)).$$

因为这个超向量的元素属于向量空间 W，且 $\boldsymbol{C}$ 为该向量空间的基，存在 $m\times n$ 矩阵 A 使得

【2.2】 $$T(\boldsymbol{B})=\boldsymbol{C}A\quad 或者\quad (T(v_1),\cdots,T(v_n))=(w_1,\cdots,w_m)\begin{bmatrix}A\end{bmatrix}$$

[第三章(4.13)]. 记住，这表明对每一 j，

【2.3】 $$T(v_j)=\sum_i w_ia_{ij}=w_1a_{1j}+\cdots+w_ma_{mj}.$$

因而 A 是以 $T(v_j)$ 的坐标向量为第 j 列构成的矩阵. 这个 $m\times n$ 矩阵 $A=(a_{ij})$ 称为 T 关于基 $\boldsymbol{B}$，$\boldsymbol{C}$ 的矩阵. 基的不同取法给出不同的矩阵.

当 $V=F^n$，$W=F^m$，且两个基都是标准基时，A 为如(2.1)构造的矩阵.

112

线性变换的矩阵可用于从 v 的坐标计算象向量 $T(v)$ 的坐标. 为此，将 v 用基表示，比如说

$$v=\boldsymbol{B}X=v_1x_1+\cdots+v_nx_n.$$

则

$$T(v)=T(v_1)x_1+\cdots+T(v_n)x_n=T(\boldsymbol{B})X=\boldsymbol{C}AX.$$

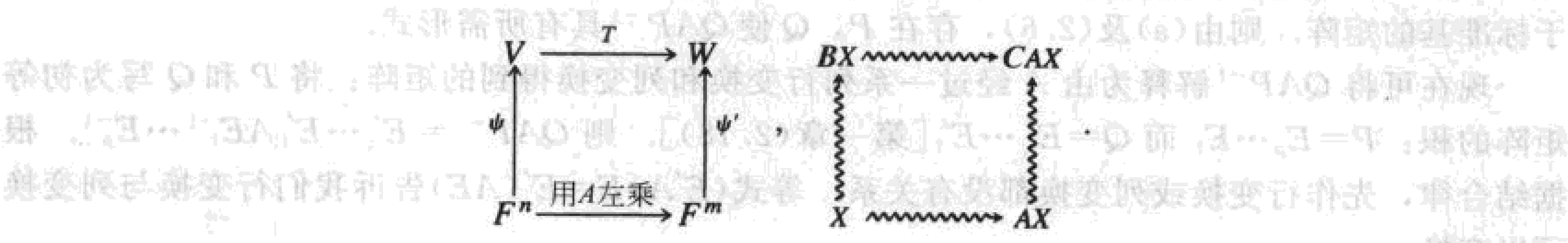
于是 $T(v)$ 的坐标向量为

$$Y=AX,$$

它是指 $T(v)=\boldsymbol{C}Y$. 换句话说，线性变换的矩阵 A 有两个对偶的性质：

【2.4】 $$T(\boldsymbol{B}) = \boldsymbol{C}A \quad 和 \quad Y = AX.$$

T 与 A 的关系可以用由两个基所确定的同构 ψ：$F^n \longrightarrow V$ 和 ψ'：$F^m \longrightarrow W$ 加以解释[第三章(4.14)]．如果用 ψ 和 ψ' 将 V 和 W 等同于 F^n 和 F^m，则 T 对应于用 A 左乘：



从此方块两个方向行进得到相同的答案：$T \circ \psi = \psi' \circ A$.

这样，一旦两个空间的基取定后，有限维向量空间 V 与 W 间的任意线性变换就可与矩阵乘法等同起来．但如果我们研究 V 和 W 中的基变换，则可以做得更好．我们要问，当选择 V 和 W 的其他基时，矩阵 A 如何变化．设 $\boldsymbol{B}' = (v'_1, \cdots, v'_n)$ 和 $\boldsymbol{C}' = (w'_1, \cdots, w'_m)$ 为 V 和 W 的新基．如第三章(4.19)，可用一个矩阵 $P \in GL_n(F)$ 将新基 $\boldsymbol{B}'$ 与旧基 $\boldsymbol{B}$ 联系起来．类似地，用矩阵 $Q \in GL_m(F)$ 将 $\boldsymbol{C}'$ 与 $\boldsymbol{C}$ 联系起来．这些矩阵具有下面的性质：

【2.5】 $$PX = X' \quad 和 \quad QY = Y'.$$

这里 X 和 X' 表示向量 $v \in V$ 关于基 $\boldsymbol{B}$ 和 $\boldsymbol{B}'$ 的坐标向量，类似地，Y 和 Y' 表示向量 $w \in W$ 关于基 $\boldsymbol{C}$ 和 $\boldsymbol{C}'$ 的坐标向量．

113

用 A' 表示 T 关于这些新基的矩阵，如上面(2.4)所定义的，于是 $A'X' = Y'$．则有 $QAP^{-1}X' = QAX = QY = Y'$．从而有

【2.6】 $$A' = QAP^{-1}.$$

注意 P 和 Q 是任意的 $n \times n$ 和 $m \times m$ 可逆矩阵[第三章(4.23)]．由此我们得到给定线性变换的矩阵的描述：

【2.7】命题 *设 A 为线性变换 T 关于给定基 $\boldsymbol{B}$，$\boldsymbol{C}$ 的矩阵．T 关于其他基的矩阵 A' 形如*

$$A' = QAP^{-1},$$

其中 $Q \in GL_m(F)$ 和 $P \in GL_n(F)$ 为任意可逆矩阵．

给定一个线性变换 T：$V \longrightarrow W$，我们自然想找到 V 和 W 的基 $\boldsymbol{B}$ 和 $\boldsymbol{C}$ 使 T 的矩阵变得特别精巧．事实上，矩阵可以化简得非常简单．

【2.8】命题

(a) *向量空间形式：设 T：$V \longrightarrow W$ 为线性变换．则可取基 $\boldsymbol{B}$，$\boldsymbol{C}$ 使 T 的矩阵具有形式*

【2.9】 $$A = \left[\begin{array}{c|c} I_r & \\ \hline & 0 \end{array}\right],$$

其中 I_r 为 $r \times r$ 单位矩阵，且 $r = \mathrm{rank} T$.

(b) *矩阵形式：给定任意 $m \times n$ 矩阵 A，存在矩阵 $Q \in GL_m(F)$ 和 $P \in GL_n(F)$ 使 QAP^{-1} 具有(2.9)形式．*

根据讨论知道两个断言都是同一回事．要从(b)推出(a)，选择任意基 $\boldsymbol{B}$，$\boldsymbol{C}$ 作为开始，设

A 是 T 关于这些基的矩阵. 应用(b)，可以找到 P，Q 使 QAP^{-1} 具有所需的形式. 如第三章(4.22)一样，令 $\mathbf{B}'=\mathbf{B}P^{-1}$ 和 $\mathbf{C}'=\mathbf{C}Q^{-1}$ 为新的基. 则 T 关于基 $\mathbf{B}'$，$\mathbf{C}'$ 的矩阵为 QAP^{-1}. 所以这些基即为所要求的. 反之，要由(a)推出(b)，可将任意矩阵 A 视为线性变换"用 A 左乘"关于标准基的矩阵. 则由(a)及(2.6)，存在 P，Q 使 QAP^{-1} 具有所需形式.

现在可将 QAP^{-1} 解释为由 A 经过一系列行变换和列变换得到的矩阵：将 P 和 Q 写为初等矩阵的积：$P=E_p\cdots E_1$ 而 $Q=E'_q\cdots E'_1$[第一章(2.18)]. 则 $QAP^{-1}=E'_q\cdots E'_1AE_1^{-1}\cdots E_p^{-1}$. 根据结合律，先作行变换或列变换都没有关系. 等式 $(E'A)E=E'(AE)$ 告诉我们行变换与列变换可以交换.

不难用矩阵乘法证明(2.8b)，但我们用基证明(2.8a). 设 $(u_1, \cdots, u_k)$ 为 $\ker T$ 的一个基. 扩张为 V 的基 $\mathbf{B}$：$(v_1, \cdots, v_r; u_1, \cdots, u_k)$，其中 $r+k=n$. 设 $w_i=T(v_i)$. 则如(1.6)的证明中所指出的，$(w_1, \cdots, w_r)$ 是 $\operatorname{im}T$ 的一个基. 扩张成 W 的基 $\mathbf{C}$：$(w_1, \cdots, w_r; x_1, \cdots, x_s)$. T 关于这些基的矩阵具有所要求的形式.

114

命题(2.8)是我们后面将证明的很多结果的原型. 因为任意线性变换的结构与一个非常简单的矩阵(2.9)相关，从而它展示了在向量空间中不用固定的基(或坐标)的威力. 因为在 F^m 上用 A 左乘是线性变换，它还告诉我们关于矩阵乘法的令人惊叹之处. 也就是说，如果使用不同的坐标系，用 A 左乘和用形如(2.9)的矩阵左乘是一样的. 因为用矩阵(2.9)左乘容易表达，我们学到了一些新的东西.

第三节 线性算子和特征向量

本节讨论一个向量空间到自身的线性变换 $T: V \longrightarrow V$. 这样的线性变换称为 V 上的线性算子. 用元素属于 F 的 $n\times n$ 矩阵左乘定义了列向量空间 F^n 的一个线性算子.

例如，平面转过角度 θ 的旋转 ρ_θ 是 $\mathbb{R}^2$ 的线性算子，它关于标准基的矩阵为

【3.1】

$$R=\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}.$$

要验证这个矩阵表示旋转，用极坐标记向量 $X\in\mathbb{R}^2$ 为 $X=(r, \alpha)$. 则其直角坐标为 $X=\begin{bmatrix}r\cos\alpha\\ r\sin\alpha\end{bmatrix}$. 正弦和余弦的加法公式指出 $RX=\begin{bmatrix}r\cos(\alpha+\theta)\\ r\sin(\alpha+\theta)\end{bmatrix}$. 这样，用极坐标表示为 $RX=(r, \alpha+\theta)$. 这表明 RX 由 X 旋转角度 θ 得到.

当讨论线性算子时，上节的讨论需作稍许改动. 显然，我们希望在 V 中只取一个基 $\mathbf{B}=(v_1, \cdots, v_n)$，用它代替第二节讨论中的 $\mathbf{B}$ 和 $\mathbf{C}$. 换言之，我们希望写出

【3.2】

$$T(\mathbf{B})=\mathbf{B}A$$

或

$$T(v_j)=\sum_i v_i a_{ij}=v_1a_{1j}+\cdots+v_na_{nj}.$$

这就定义了 T 的矩阵 $A=(a_{ij})$. 它是一个方阵，其第 j 列是 $T(v_j)$ 关于基 $\mathbf{B}$ 的坐标向量. 如果用 V 和 $\mathbf{B}$ 代替 W 和 $\mathbf{C}$，式(2.4)不变. 如上节一样，如果用 X 和 Y 分别表示 v 与 $T(v)$ 的坐标向量，则有

115

【3.3】
$$Y = AX.$$

当我们研究 V 上的基变换的效果时，产生了新的特性．假设用一组新基 $\mathbf{B}' = (v'_1, \cdots, v'_n)$ 代替 $\mathbf{B}$．则式(2.7)显示新矩阵 A' 具有

【3.4】
$$A' = PAP^{-1}$$

的形式，其中 P 为基变换的矩阵．这样，线性变换中基变换的规则由下列规则代替：

【3.5】命题　设 A 是一个线性算子 T 关于一个基 $\mathbf{B}$ 的矩阵．对于不同的基，代表 T 的矩阵具有形式

$$A' = PAP^{-1},$$

其中 $P \in GL_n(F)$ 是任意矩阵．

一般地，如果有矩阵 $P \in GL_n(F)$ 使 $A' = PAP^{-1}$，我们说方阵 A 与 A' 相似．也可以使用共轭这个词[见第二章(3.4)]．

给定 A，自然要求特别简单的相似矩阵 A'．也许可以期待一个类似(2.10)的结果．但我们这里允许的变换有更多限制，因为只有一个基，从而只有一个矩阵 P 可用．

把假设的矩阵 P 写成初等矩阵的积：$P = E_r \cdots E_1$，可以对问题有一些领悟．这时

$$PAP^{-1} = E_r \cdots E_1 A E_1^{-1} \cdots E_r^{-1}.$$

用初等变换的语言，可以通过一系列步骤 $A \rightsquigarrow EAE^{-1}$ 改变 A．换言之，可以作任意行变换 E，但随后必须也作一个其逆的列变换 E^{-1}．可是，行变换与列变换互相干扰，这使得不能直接分析这些作用的效果．我不知道如何使用它们．值得一提的是，其中大部分都可以用别的办法加以解决．

分析线性算子的主要工具是特征向量和不变子空间的概念．

设 $T: V \longrightarrow V$ 是向量空间的线性算子．V 的一个子空间 W 称为不变子空间或 T-不变子空间，如果它在算子 T 的作用下变到自身：

【3.6】
$$TW \subset W.$$

换言之，若对所有 $w \in W$ 有 $T(w) \in W$，则 W 是 T-不变的．当 W 为 T-不变的时，T 在 W 上定义一个线性算子，称为 T 在 W 上的限制．

设 W 为 T-不变子空间，我们选择 V 的一个基 $\mathbf{B}$，它由在 W 的一个基$(w_1, \cdots, w_k)$上添加向量而得到：

$$\mathbf{B} = (w_1, \cdots, w_k, v_1, \cdots, v_{n-k}).$$

则 W 是不变子空间这一事实可以从 T 的矩阵 M 中看出来．因为这个矩阵的列为象向量的坐标向量[见(2.3)]，而 $T(w_j)$ 属于子空间 W，从而它是基$(w_1, \cdots, w_k)$的线性组合．因此，当我们把 $T(w_j)$ 用基 $\mathbf{B}$ 表出时，向量 $v_1, \cdots, v_{n-k}$ 的系数为零．由此，矩阵 M 具有分块形式

116

【3.7】
$$M = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}.$$

其中 A 为 $k \times k$ 矩阵．而且，A 是 T 在 W 上的限制的矩阵．

假设 $V = W_1 \oplus W_2$ 为两个 T-不变子空间的直和，并设 $\mathbf{B}_i$ 为 W_i 的一个基．则将 $\mathbf{B}_1$ 和 $\mathbf{B}_2$ 的元素顺序排起来，可以构成 V 的一个基 $\mathbf{B}$[第三章(6.6a)]．这时，T 的矩阵为分块对角形式

【3.8】
$$M=\begin{bmatrix}A_1 & 0\\ 0 & A_2\end{bmatrix},$$
其中，A_i 是 T 在 W_i 上的限制的矩阵.

特征向量的概念与不变子空间的概念是紧密联系的. 线性算子 T 的特征向量 v 是对某个常数$c\in F$，满足条件

【3.9】
$$T(v)=cv$$
的非零向量. 这里，c 可以取 0，但向量 v 不能为 0. 从几何上看，若 $V=\mathbb{R}^n$，特征向量 v 是与 $T(v)$平行的非零向量.

(3.9)中的标量 c 称为与特征向量 v 对应的特征值. 当我们说到线性算子 T 的特征值时，指的是一个标量 $c\in F$，它是与某个特征向量对应的特征值.

例如，标准基向量 e_1 是矩阵
$$\begin{bmatrix}3 & 1\\ 0 & 2\end{bmatrix}$$
左乘的特征向量，与特征向量 e_1 对应的特征值是 3. 另外，向量(0，1，1)' 是用矩阵
$$A=\begin{bmatrix}1 & 1 & -1\\ 2 & 1 & 1\\ 3 & 0 & 2\end{bmatrix}$$
左乘列向量空间$\mathbb{R}^3$ 的特征向量，其特征值是 2.

有时，特征向量和特征值也称为*本征向量*和*本征值*.

设 v 是线性算子 T 的特征向量. 由 v 张成的子空间 W 是 T-不变的，因为对所有 $a\in F$，

117

$T(av)=acv\in W$. 反之，若这个空间不变，则 v 是特征向量. 因而，特征向量可以描述为一维 T-不变子空间的基. 若 v 是特征向量，且将它扩张为 V 的一个基($v=v_1$，…，v_n)，则矩阵 T 将有分块形式
$$\begin{bmatrix}c & B\\ 0 & D\end{bmatrix}=\left[\begin{array}{c|ccc}c & * & \cdots & *\\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right],$$
其中 c 是 v 的特征值. 这是块分解(3.7)关于 1 维不变子空间的情形.

我们说 $n\times n$ 矩阵 A 的特征向量时，是指用 A 左乘的特征向量，即满足条件
$$AX=cX,\quad 对某个\ c\in F$$
的非零列向量. 像前面一样，标量 c 称为特征值，设 A 是 T 关于基 $\boldsymbol{B}$ 的矩阵，X 表示向量 $v\in V$ 的坐标向量. 则 $T(v)$的坐标向量是 AX[(2.4)]. 因而，X 是 A 的特征向量当且仅当 v 是 T 的特征向量. 而且，如果这一点成立，则特征值相等：T 与 A 有相同的特征值.

【3.10】推论 相似矩阵有相同的特征值.

这可由事实(3.5)——相似矩阵代表同一线性变换得到.

特征向量并不总是容易找到的，但容易看出一个给定向量 X 是否是矩阵 A 的特征向量. 我们只需验证 AX 是否是 X 的倍数就行了. 因此，如果关于一个基，v 的坐标向量及 T 的矩

阵给出后，我们就能知道向量 v 是否是线性算子 T 的特征向量. 如果考虑一个基向量，就得到下面的判别法：

【3.11】 基向量 v_j 是 T(具有特征值 c)的一个特征向量当且仅当 A 的第 j 列具有 ce_j 的形式.

因为矩阵 A 由性质 $T(v_j)=v_1a_{1j}+\cdots+v_na_{nj}$ 定义. 于是，若 $T(v_j)=cv_j$，则 $a_{jj}=c$ 且当 $i\neq j$ 时，$a_{ij}=0$.

【3.12】推论 用上面的记号，A 是对角矩阵当且仅当每一个基向量 v_j 皆为特征向量.

【3.13】推论 线性变换的矩阵 A 与对角矩阵相似当且仅当存在由特征向量构成的 V 的基 $\boldsymbol{B}'=(v'_1,\cdots,v'_n)$.

118

后一个推论指出，如果有足够多的特征向量，可以把一个线性算子用对角矩阵简单地表出. 在第四节我们将看到复向量空间的任一线性算子至少有一个特征向量，在第六节将看到在大部分情形特征向量构成一个基. 但实向量空间的线性算子不一定有特征向量. 例如，(3.1)平面的旋转 ρ_θ，除非 $\theta=0$ 或 π，否则不会把任何一个向量变换到与其平行的向量. 因此，除了 $\theta=0$ 或 π 的情形外，ρ_θ 没有特征向量.

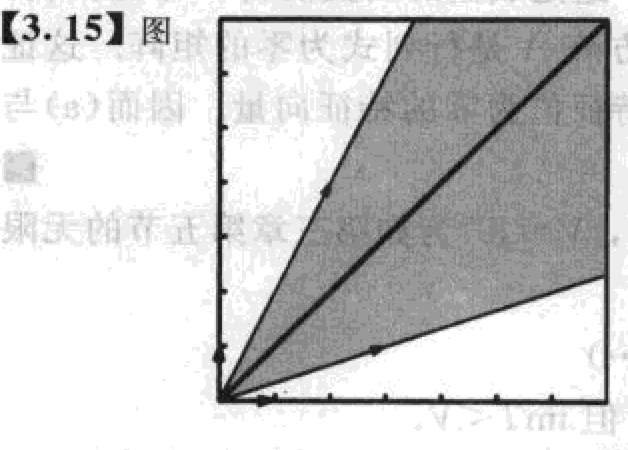
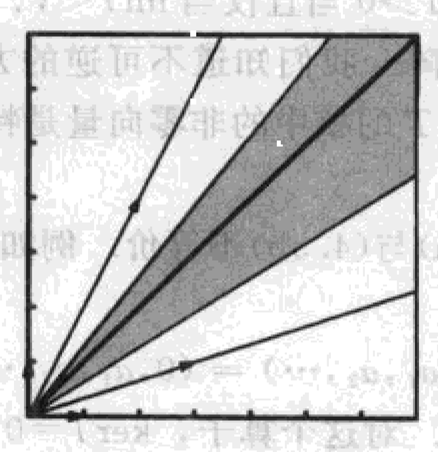
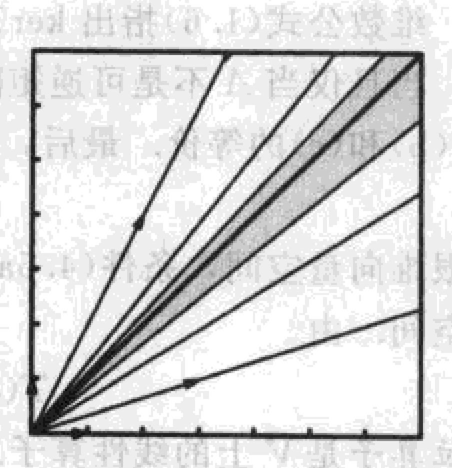
具有正元素的实矩阵的情形就大不一样. 这样的矩阵有时称为正矩阵. 它们在应用中经常出现，其最重要的性质之一是总有一个坐标为正数的特征向量(正特征向量). 我们不证明这个事实，而是通过考察在$\mathbb{R}^2$ 上正 2×2 矩阵 A 乘法的作用来加以说明.

设 $w_i=Ae_i$. 向量加法的平行四边形法则指出，A 将第一象限 S 映到向量 w_1，w_2 所界定的扇形. 而 w_i 的坐标向量是 A 的第 i 列. 因为 A 的元素都是正的，w_i 都在第一象限中. 从而 A 把第一象限映到第一象限：$S\supset AS$. 再用 A 作用，得 $AS\supset A^2S$，继续下去，有

【3.14】
$$S\supset AS\supset A^2S\supset A^3S\supset\cdots,$$

当矩阵 $A=\begin{bmatrix}3&2\\1&4\end{bmatrix}$时，如下面图(3.15)所示.

【3.15】图

第一象限在正矩阵不断乘积之下的象

这样扇形套的交或为一个扇形或为一条半直线. 这里，交 $Z=\bigcap A^rs$ 为半直线. 从直观上看这是合理的，也可以用各种方法来证明. 证明留作练习. 我们在关系 $Z=\bigcap A^rS$ 的两边用 A 乘，得到

$$AZ=A\Big(\bigcap_0^\infty A^rS\Big)=\bigcap_1^\infty A^rS=Z.$$

因而 $Z=AZ$. 这就证明了 Z 中的非零向量是特征向量.

119

第四节 特征多项式

本节我们确定任意线性算子 T 的特征向量. 我们先回顾一下, T 的特征向量是满足条件

【4.1】 $$T(v)=cv$$

对某个 $c\in F$ 成立的非零向量 v. 乍一看, 如果线性算子相应的矩阵很复杂, 似乎很难求出其特征向量. 诀窍是转而解决另一个问题, 即先求特征值. 当特征值 c 确定后, 方程(4.1)成为 v 的坐标的线性方程组, 对其求解是没有问题的.

首先, 将(4.1)写为形式

【4.2】 $$[T-cI](v)=0,$$

其中 I 为恒等算子, 而 $T-cI$ 是由

【4.3】 $$[T-cI](v)=T(v)-cv$$

定义的线性算子. 容易验证 $T-cI$ 的确是线性算子. 若 T 关于某个基的矩阵为 A, 则 $T-cI$ 的矩阵是 $A-cI$.

(4.2)可复述为

【4.4】 v 在 $T-cI$ 的核中.

【4.5】引理 对有限维向量空间上的线性算子 $T: V\longrightarrow V$, 下列条件等价:

(a) $\ker T>0$.

(b) $\operatorname{im} T<V$.

(c) 若 A 是算子关于任意基的矩阵, 则 $\det A=0$.

(d) 0 是 T 的一个特征值.

证明 维数公式(1.6)指出 $\ker T>0$ 当且仅当 $\operatorname{im} T<V$. 这是成立的当且仅当 T 不是同构, 或等价地, 当且仅当 A 不是可逆矩阵. 我们知道不可逆的方阵 A 是行列式为零的矩阵. 这证明了(a)、(b)和(c)的等价. 最后, T 的核中的非零向量是特征值为零的特征向量. 因而(a)与(d)等价. ■

对无限维向量空间, 条件(4.5a)与(4.5b)不等价. 例如, $V=\mathbb{R}^\infty$ 为如第三章第五节的无限维行向量空间. 由

【4.6】 $$T(a_1,a_2,\cdots)=(0,a_1,a_2,\cdots)$$

120 定义的移位算子是 V 上的线性算子. 对这个算子, $\ker T=0$ 但 $\operatorname{im} T<V$.

【4.7】定义 有限维向量空间 V 的线性算子 T, 如果满足(4.5)中的任一等价条件, 则称之为**奇异的**. 否则, 称之为**非奇异的**.

我们知道, c 是算子 T 的一个特征值当且仅当 $T-cI$ 有非零核(4.4). 因此, 如果在上面的引理中用 $T-cI$ 代替 T, 我们得到下面的推论.

【4.8】推论 线性算子 T 的特征值是使得 $T-cI$ 奇异的标量 $c\in F$.

若 A 是 T 关于某个基的矩阵, 则 $T-cI$ 的矩阵为 $A-cI$. 因而 $T-cI$ 奇异当且仅当 $\det(A-cI)=0$. 这个行列式可以具体地算出来, 并且这给我们提供一个确定特征值和特征向量的具体方法.

例如，假设 A 为矩阵

【4.9】
$$\begin{bmatrix}3 & 2\\1 & 4\end{bmatrix},$$

它在$\mathbb{R}^2$ 上的作用如图(3.15)所示. 则

$$A-cI=\begin{bmatrix}3 & 2\\1 & 4\end{bmatrix}-\begin{bmatrix}c & 0\\0 & c\end{bmatrix}=\begin{bmatrix}3-c & 2\\1 & 4-c\end{bmatrix}$$

且

$$\det(A-cI)=c^2-7c+10=(c-5)(c-2).$$

如果 $c=5$ 或 2 则行列式为零，于是证明了 A 的特征值为 5 或 2. 要想求特征向量，解两个线性方程组$[A-5I]X=0$ 和$[A-2I]X=0$. 其解在不计标量因子时是唯一的：

【4.10】
$$v_1=\begin{bmatrix}1\\1\end{bmatrix},\quad v_2=\begin{bmatrix}2\\-1\end{bmatrix}.$$

注意，特征值为 5 的特征向量 v_1 属于第一向限. 它位于图(3.15)所示的半直线 Z 之上.

现在我们对任意矩阵作同样的计算. 改变符号会方便一些. 显然 $\det(cI-A)=0$ 当且仅当 $\det(A-cI)=0$. 而且，习惯上用变量 t 代替符号 c. 构造矩阵 $tI-A$：

【4.11】
$$tI-A=\begin{bmatrix}(t-a_{11}) & -a_{12} & \cdots & -a_{1n}\\ -a_{21} & (t-a_{22}) & \cdots & -a_{2n}\\ \vdots & & & \vdots\\ -a_{n1} & \cdots & \cdots & (t-a_{nn})\end{bmatrix}.$$

于是，行列式的完全展开[第一章(4.11)]指出 $\det(tI-A)$是 t 的 n 次多项式，其系数为标量.

121

【4.12】定义 线性算子 T 的**特征多项式**是

$$p(t)=\det(tI-A),$$

其中 A 是 T 关于某个基的矩阵.

(4.8)与(4.12)合起来确定 T 的特征值：c 是特征值当且仅当 $p(c)=0$.

【4.13】推论 线性算子的特征值是其特征多项式的根.

【4.14】推论 上三角矩阵或下三角矩阵的特征值为其对角元.

证明 如果 A 是上三角矩阵，则 $tI-A$ 也是. 三角矩阵的行列式为其对角元的积，而 $tI-A$的对角元为 $t-a_{ii}$. 因而，特征多项式是 $p(t)=(t-a_{11})(t-a_{22})\cdots(t-a_{nn})$，且它的根——特征值为 a_{11}，…，a_{nn}. ■

我们可以毫无困难地计算任意 2×2 矩阵

$$A=\begin{bmatrix}a & b\\c & d\end{bmatrix}$$

的特征多项式. 它是

【4.15】
$$\det(tI-A)=\det\begin{bmatrix}t-a & -b\\-c & t-d\end{bmatrix}=t^2-(a+d)t+(ad-bc).$$

这个多项式的判别式为

【4.16】 $$(a+d)^2-4(ad-bc)=(a-d)^2+4bc.$$

如果 A 的元为正实数，则判别式也为正，从而如第三节最后所预测的，特征多项式有实根.

【4.17】命题 算子 T 的特征多项式与基的选择无关.

证明 第二个基相应的矩阵为 $A'=PAP^{-1}$[见(3.4)]. 我们有

$$tI-A'=tI-PAP^{-1}=P(tI)P^{-1}-PAP^{-1}=P(tI-A)P^{-1}.$$

于是

$$\det(tI-A')=\det(P(tI-A)P^{-1})=\det P\det(tI-A)\det P^{-1}=\det(tI-A).$$

122 因此，用 A 和 A' 计算得到的特征多项式相等，这正是所断言的. ■

【4.18】命题 特征多项式 $p(t)$ 具有

$$p(t)=t^n-(\mathrm{tr}\ A)t^{n-1}+(\text{中间项})+(-1)^n(\det A)$$

的形式，其中，A 的**迹** $\mathrm{tr}A$ 是对角元的和

$$\mathrm{tr}\ A=a_{11}+a_{22}+\cdots+a_{nn}.$$

所有的系数与基无关. 例如，$\mathrm{tr}\ PAP^{-1}=\mathrm{tr}\ A$.

这可通过计算来证明. 与基无关这一性质由(4.17)得到.

因为特征多项式、迹和行列式都是与基无关的，它们仅依赖于算子 T，故可以将线性算子 T 的特征多项式、迹和行列式定义为由 T 关于任意基的矩阵所得到的.

【4.19】命题 设 T 是有限维向量空间 V 的线性算子.

(a) 若 V 的维数为 n，则 T 最多有 n 个特征值.

(b) 若 F 为复数域且 $V\neq 0$，则 T 至少有一个特征值，因而它有一个特征向量.

证明

(a) n 次多项式最多有 n 个不同的根. 虽然我们还没有证明这一点[见第十一章(1.8)]，但这对任意域 F 都是成立的. 这样，可以应用(4.13).

(b) 每一复系数的正次数多项式至少有一个复根. 这个事实称为代数基本定理，在第十三章(9.1)有一个证明. ■

例如，设 A 为实平面$\mathbb{R}^2$ 上转过角度 θ 的旋转(3.1). 其特征多项式为

【4.20】 $$p(t)=t^2-(2\cos\theta)t+1,$$

除了 $\cos\theta=\pm1$ 外它没有实根. 但若视 A 为$\mathbb{C}^2$ 上的算子，则它有两个复特征值.

第五节 正交矩阵与旋转

本节将把二、三维空间$\mathbb{R}^2$ 和$\mathbb{R}^3$ 绕原点的旋转作为线性算子进行描述. 在(3.1)中，我们已注意到$\mathbb{R}^2$ 上转过角度 θ 的旋转可用矩阵

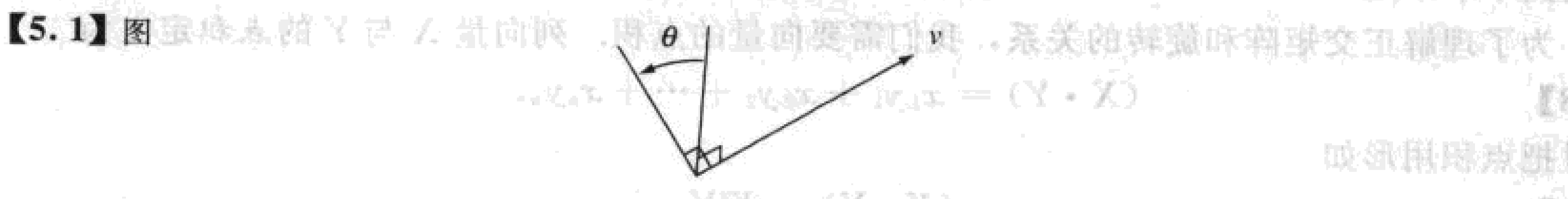
$$\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}$$

123 乘来表示.

$\mathbb{R}^3$ 关于原点的旋转可用一对(v,θ)来刻画，这个对由单位向量 v、位于旋转轴上的长度为

1 的向量，以及非零角度 θ、旋转的角度组成. 两个对 (v, θ) 和 $(-v, -\theta)$ 代表同一个旋转. 我们把恒等映射也看作一个旋转，虽然其旋转轴是未定的.

【5.1】图



容易由 2×2 旋转矩阵得到绕向量 e_1 转过角度 θ 的旋转的矩阵表示，即

【5.2】
$$A=\begin{bmatrix}1 & 0 & 0\\ 0 & \cos\theta & -\sin\theta\\ 0 & \sin\theta & \cos\theta\end{bmatrix}.$$

用 A 乘固定向量的第一个坐标 x_1，而在 $(x_2, x_3)^t$ 上是旋转作用. $\mathbb{R}^3$ 的所有绕原点的旋转都是线性算子，但其矩阵相当复杂. 本节的目的是刻画这些旋转矩阵.

一个实 $n\times n$ 矩阵 A 称为*正交的*，如果 $A^t=A^{-1}$，或等价地 $A^tA=I$. 所有正交 $n\times n$ 矩阵构成 $GL_n(\mathbb{R})$ 的一个子群，记为 O_n，称为*正交群*：

【5.3】
$$O_n=\{A\in GL_n(\mathbb{R})\mid A^tA=I\}.$$

正交矩阵的行列式为 ±1，这是因为，如果 $A^tA=I$，则

$$(\det A)^2=(\det A^t)(\det A)=1.$$

具有行列式 $+1$ 的正交矩阵构成一个子群，称为*特殊正交群*，记作 SO_n：

【5.4】
$$SO_n=\{A\in GL_n(\mathbb{R})\mid A^tA=I, \det A=1\}.$$

除了 SO_n，这个子群还有一个陪集，即行列式为 -1 的元素的集合. 故它在 O_n 中的指标为 2.

关于旋转，我们将证明的主要事实叙述如下.

【5.5】定理 *$\mathbb{R}^2$ 或 $\mathbb{R}^3$ 绕原点的旋转是线性算子，它们关于标准基的矩阵是正交的，且行列式为 1. 换言之，矩阵 A 代表 $\mathbb{R}^2$（或 $\mathbb{R}^3$）的旋转当且仅当 $A\in SO_2$（或 SO_3）.*

注意下面的推论：

【5.6】推论 *$\mathbb{R}^3$ 中两个绕原点的旋转的合成仍是一个旋转.*

124

推论可由定理得到，因为代表两个线性算子合成的矩阵是积矩阵，而作为 $GL_3(\mathbb{R})$ 的子群，SO_3 在积下封闭. 从几何上说，这是很不明显的. 显然，绕同一轴的两个旋转的合成是绕同一轴的旋转. 但想象绕不同轴的旋转. 合成算子的旋转轴是什么？

因为其元素为旋转，群 SO_2 和 SO_3 分别称为二、三维*旋转群*. 维数 >3 时将更复杂. 例如，矩阵

【5.7】
$$\begin{bmatrix}\cos\theta & -\sin\theta & & \\ \sin\theta & \cos\theta & & \\ & & \cos\eta & -\sin\eta\\ & & \sin\eta & \cos\eta\end{bmatrix}$$

为 SO_4 的一个元素. 这个矩阵左乘是前两个坐标的一个 θ 角度旋转和后两个坐标的一个 η 角度旋转的合成. 这样的作用不能用单个旋转实现.

定理(5.5)的证明并不太难，但如果不先引入一些术语，它将很繁琐．因而我们将其证明推迟到本节末尾．

为了理解正交矩阵和旋转的关系，我们需要向量的点积．列向量 X 与 Y 的*点积*定义为

【5.8】
$$(X\cdot Y)=x_1y_1+x_2y_2+\cdots+x_ny_n.$$

有时把点积用形如

【5.9】
$$(X\cdot Y)=X^tY$$

的矩阵形式写出很有用．

$\mathbb{R}^2$ 和 $\mathbb{R}^3$ 中向量的点积有两个主要性质．第一个性质是 $(X\cdot X)$ 是向量长度的平方，根据不同的情形，有

$$|X|^2=x_1^2+x_2^2 \quad 或 \quad x_1^2+x_2^2+x_3^2.$$

这一性质(可以由毕达哥拉斯定理推出)是定义 $\mathbb{R}^n$ 中向量长度的基础：X 的长度由公式

【5.10】
$$|X|^2=(X\cdot X)=x_1^2+\cdots+x_n^2$$

定义．两个向量 X，Y 间的距离定义为 $X-Y$ 的长度 $|X-Y|$．

$\mathbb{R}^2$ 和 $\mathbb{R}^3$ 中向量的点积的第二个重要性质是公式

125

【5.11】
$$(X\cdot Y)=|X||Y|\cos\theta,$$

其中 θ 是向量间的夹角．这个公式是边长为 a，b，c 的三角形余弦法则

$$c^2=a^2+b^2-2ab\cos\theta$$

的结果，其中 θ 是 a，b 边的夹角．要导出(5.11)，对顶点为 0，X，Y 的三角形应用余弦法则．其边长为 $|X|$，$|Y|$ 和 $|X-Y|$，因此余弦法则可写为

$$(X-Y\cdot X-Y)=(X\cdot X)+(Y\cdot Y)-2|X||Y|\cos\theta.$$

左边展开得

$$(X-Y\cdot X-Y)=(X\cdot X)-2(X\cdot Y)+(Y\cdot Y),$$

比较两边得(5.11)．

(5.11)的最重要应用是两个向量 X 和 Y 正交，这是指其夹角为 $\frac{\pi}{2}$，当且仅当 $(X\cdot Y)=0$．这一性质被用来作为 $\mathbb{R}^n$ 中向量正交的定义：

【5.12】 *X 与 Y 正交，如果 $(X\cdot Y)=0$.*

【5.13】命题 *对实 $n\times n$ 矩阵 A，下列条件等价：*

(a) A 是正交的．

(b) 用 A 乘保持点积，即对列向量 X，Y 有 $(AX\cdot AY)=(X\cdot Y)$．

(c) A 的列是互相正交的单位向量．

由互相正交的单位向量构成的基称为*标准正交基*．正交矩阵是其列向量构成标准正交基的矩阵．

用正交矩阵左乘也称为*正交算子*．这样，$\mathbb{R}^n$ 的正交算子是保持点积的线性算子．

命题(5.13)的证明 我们记 $(X\cdot Y)=X^tY$．若 A 正交，则 $A^tA=I$，于是

$$(X\cdot Y)=X^tY=X^tA^tAY=(AX)^t(AY)=(AX\cdot AY).$$

反之，假设对所有 X 和 Y，有 $X^tY=X^tA^tAY$．将该等式重新写为 $X^tBY=0$，其中 $B=I-$

A^tA. 对任意矩阵 B，有

【5.14】 $$e_i^tBe_j = b_{ij}.$$

于是，若对所有 X，Y 有 $X^tBY=0$，则 $e_i^tBe_j=b_{ij}=0$ 对所有 i，j 成立，且 $B=0$. 从而 $I=A^tA$. 这就证明了(a)与(b)等价. 要证(a)与(c)等价，用 A_j 记矩阵 A 的第 j 列. 积矩阵 A^tA 的(i, j)项是$(A_i \cdot A_j)$. 于是，$A^tA=I$ 当且仅当对所有 i，有$(A_i \cdot A_i)=1$，且对所有 $i \neq j$，有$(A_i \cdot A_j)=0$，这就是说，列向量长度为 1 且是正交的. ■ 126

用正交矩阵左乘的几何意义可以用刚体运动这一术语解释. $\mathbb{R}^n$ 的*刚体运动*或*等距*是一个保持距离的映射 m：$\mathbb{R}^n \longrightarrow \mathbb{R}^n$，即它是满足下列条件的映射：若 X，Y 是$\mathbb{R}^n$ 的点，则由 X 到 Y 的距离等于由 $m(X)$到 $m(Y)$的距离：

【5.15】 $$|m(X)-m(Y)| = |X-Y|.$$

这样的刚体运动将三角形映到全等的三角形，因而一般来说，它保持角度和形状.

注意，两个刚体运动的合成是刚体运动，而且刚体运动的逆也是刚体运动. 因而，$\mathbb{R}^n$ 的刚体运动对于作用的合成法则构成一个群 M_n. 这个群称为*运动群*.

【5.16】命题 *设 m 是一个映射$\mathbb{R}^n \longrightarrow \mathbb{R}^n$. 则下列关于 m 的条件等价：*

(a) m 是一个固定原点的刚体运动.

(b) m 保持点积，即对所有 X，$Y \in \mathbb{R}^n$，$(m(X) \cdot m(Y))=(X \cdot Y)$.

(c) m 是一个正交矩阵的左乘.

【5.17】推论 *固定原点的刚体运动是线性算子.*

这可由(a)与(c)等价得到.

命题(5.16)的证明 我们用简写$'$表示映射 m，记 $m(X)=X'$. 设 m 是固定原点的刚体运动. 对所有向量 X，Y 用简写记号，m 保持距离的(5.15)改写为

【5.18】 $$(X'-Y' \cdot X'-Y') = (X-Y \cdot X-Y).$$

取 $Y=0$，得到$(X' \cdot X')=(X \cdot X)$对所有 X 成立. 展开(5.18)的两边，消去项$(X \cdot X)$和$(Y \cdot Y)$，得$(X' \cdot Y')=(X \cdot Y)$. 这说明 m 保持点积，于是(a)推出(b).

要证(b)推出(c)，注意保持点积且固定所有的基向量 e_i 的唯一映射是恒等映射. 这是因为，若 m 保持点积，则对任意 X，$(X \cdot e_j)=(X' \cdot e_j')$. 若还有 $e_j'=e_j$，则

$$x_j = (X \cdot e_j) = (X' \cdot e'_j) = (X' \cdot e_j) = x'_j$$

对所有 j 成立. 于是 $X=X'$且 m 为恒等映射.

现设 m 保持点积. 则标准基向量的象 e'_1，…，e'_n 是标准正交基：$(e'_i \cdot e'_i)=1$，且如果 $i \neq j$，$(e'_i \cdot e'_j)=0$. 设 $\boldsymbol{B}'=(e'_1, \cdots, e'_n)$，并设 $A=[\boldsymbol{B}']$. 由命题(5.13)，A 是一个正交矩阵. 由于正交矩阵构成一个群，A^{-1}亦正交. 这样，用 A^{-1}左乘亦保持点积. 从而合成运动 $A^{-1}m$ 保持点积，且它固定每一基向量 e_i. 从而 $A^{-1}m$ 为恒等映射. 这证明 m 为用 A 左乘，正是我们要证的. 127

最后，如果 m 是线性算子，其矩阵 A 正交，则由于 m 是线性的，$X'-Y'=(X-Y)'$，且由(b)，$|X'-Y'|=|(X-Y)'|=|X-Y|$. 因而，m 是刚体运动. 因为线性算子也固定 0，这表明(c)推出(a). ■

一类不固定原点因而不是线性算子的刚体运动是平移. 给出任意$\mathbb{R}^n$ 中固定的向量 $b=$

$(b_1, \cdots, b_n)^t$，用 b 平移是映射

【5.19】
$$t_b(X) = X + b = \begin{bmatrix} x_1 + b_1 \\ \vdots \\ x_n + b_n \end{bmatrix}.$$

这个映射为刚体运动，因为 $t_b(X) - t_b(Y) = (X+b) - (Y+b) = X - Y$，故 $|t_b(X) - t_b(Y)| = |X - Y|$.

【5.20】命题 每一刚体运动 m 是一个正交线性算子和一个平移的合成．换句话说，对某个正交矩阵 A 和向量 b，它具有 $m(X) = AX + b$ 的形式．

证明 设 $b = m(0)$．则 $t_{-b}(b) = 0$，于是合成的作用 $t_{-b}m$ 是固定原点的刚体运动：$t_{-b}(m(0)) = 0$．根据命题(5.16)，$t_{-b}m$ 是用正交矩阵 A 左乘：$t_{-b}m(X) = AX$．在方程的两边同时用 t_b 作用，我们得 $m(X) = AX + b$.

注意，向量 b 和矩阵 A 都由 m 唯一确定，因为 $b = m(0)$ 而 A 是算子 $t_{-b}m$. ■

记住正交矩阵的行列式为 ± 1．如果行列式为 $+1$，称正交算子为保向的，如果行列式为 -1，称正交算子为反向的．同样，设 m 为一个刚体运动．记 $m(X) = AX + b$．如果 $\det A = 1$，则称 m 为保向的，而如果 $\det A = -1$，则称 m 为反向的．$\mathbb{R}^2$ 的一个运动，如果它翻转平面，则它为反向的，否则为保向的．

定理(5.5)和命题(5.16)合起来，给出了旋转的下面推论．

【5.21】推论 $\mathbb{R}^2$ 和 $\mathbb{R}^3$ 的旋转为固定原点的保向刚体运动．

我们现在着手证明定理(5.5)，它刻画了 $\mathbb{R}^2$ 和 $\mathbb{R}^3$ 绕原点的旋转．每一个旋转 ρ 是一个刚体运动，因此命题(5.16)告诉我们，ρ 是用正交矩阵 A 左乘．另外，A 的行列式为 1．这是因为，对任意正交矩阵，$\det A = \pm 1$，而且行列式随旋转角度连续变化．当角度为 0 时，A 为恒等矩阵，其行列式为 1．这样，旋转的矩阵为 SO_2 或 SO_3 的一个元素．

128

反之，设 $A \in SO_2$ 为一个正交 2×2 矩阵，行列式为 1．设 v_1 为 A 的第一个列向量 Ae_1．由于 A 是正交的，v_1 为一个单位向量．存在一个旋转 R(3.1)使 $Re_1 = v_1$．于是 $B = R^{-1}A$ 固定 e_1．另外，A 和 R 都是 SO_2 的元素，这意味着 B 也属于 SO_2．因而，B 的列向量构成 $\mathbb{R}^2$ 的标准正交基，且第一列为 e_1．由于长度为 1 且与 e_1 正交，故第二列必为 e_2 或 $-e_2$，而第二种情形由 $\det B = 1$ 这一事实排除，故得到 $B = I$ 且 $A = R$．从而 A 是旋转．

要证 SO_3 的元素 A 代表旋转，最好明确 $\mathbb{R}^3$ 关于原点的旋转 ρ 的定义．我们将需要下列条件．

【5.22】

(i) ρ 是固定原点的刚体运动．

(ii) ρ 还固定一个非零向量 v．

(iii) ρ 在与 v 垂直的平面上作用为旋转．

根据命题(5.16)，第一个条件等价于说 ρ 是正交算子．故矩阵 $A \in SO_3$ 满足这一条件．条件(ii)可以叙述为 v 是一个特征值为 1 的特征向量，于是由于 ρ 保持正交性，它将正交空间 P 映到自身．换言之，P 是不变子空间．条件(iii)说 ρ 在这个不变子空间的限制是一个旋转．

注意矩阵(5.2)的确满足这些条件，其中 $v=e_1$.

【5.23】引理 每个元素 $A\in SO_3$ 都有特征值 1.

证明 我们将证 $\det(A-I)=0$. 这样就证明了该引理[见(4.8)]. 证明是巧妙的，但很高效. 回忆 $\det A=\det A^t$ 对任意矩阵 A 成立，于是 $\det A^t=1$. 因为 A 正交，所以 $A^t(A-I)=(I-A)^t$. 于是

$$\begin{aligned}\det(A-I)&=\det A^t(A-I)\\&=\det(I-A)^t\\&=\det(I-A).\end{aligned}$$

另一方面，对任意 3×3 矩阵 B，$\det(-B)=-\det B$. 从而有 $\det(A-I)=-\det(I-A)$，由此得 $\det(A-I)=0$. ■

给定一个矩阵 $A\in SO_3$，上述引理指出用 A 左乘固定一个非零向量 v_1. 将其长度规范为 1，而且选择位于与 v_1 正交的平面 P 中的正交单位向量 v_2，v_3，则 $\boldsymbol{B}=(v_1, v_2, v_3)$是$\mathbb{R}^3$ 的标准正交基. 因为矩阵$[\boldsymbol{B}]$为正交的，所以矩阵 $P=[\boldsymbol{B}]^{-1}$是正交的，且 $A'=PAP^{-1}$关于基 $\boldsymbol{B}$ 与 A 表示同一个变换. 因为 A 和 P 皆正交，所以 A'也正交. 又 $\det A'=\det A=1$. 因此，$A'\in SO_3$. [129]

因为 v_1 是特征值为 1 的特征向量，A'的第一列为 e_1. 因 A'正交，故其他列与 e_1 正交，且 A'具有块形式

$$\left[\begin{array}{c|c}1&0\\\hline 0&R\end{array}\right],$$

利用 $A'\in SO_3$ 这一事实，我们得到 $R\in SO_2$. 因此 R 是旋转. 这表明 A'具有(5.2)形式并且表示旋转. 因而 A 也表示旋转. 这就完成了定理(5.5)的证明.

【5.24】注 为了将新基与旧基区分开，在第三章中我们把它记作 $\boldsymbol{B}'$. 当旧基为标准基时，撇是可以不要的，由于撇使得记号凌乱，所以我们常把它去掉，正如这里一样.

第六节 对角化

本节证明对“大多数”复向量空间的线性算子，存在一个基，使得算子的矩阵是对角的. 其关键事实我们在第四节的结尾处已注意到，即每一个正次数的复多项式都有一个根. 这表明每个线性算子都有一个特征向量.

【6.1】命题

(a) 向量空间形式：设 T 是有限维复向量空间 V 上的线性算子. 存在 V 的基 $\boldsymbol{B}$，使得 T 的矩阵为上三角的.

(b) 矩阵形式：每一个 $n\times n$ 复矩阵 A 相似于一个上三角矩阵. 换言之，存在矩阵 $P\in GL_n(\mathbb{C})$，使得 PAP^{-1}为上三角的.

证明 由(3.5)，两个断言是等价的. 我们首先应用(4.19b)，这表明存在一个特征向量，称之为 v'_1. 扩张为 V 的一个基 $\boldsymbol{B}'=(v'_1, \cdots, v'_n)$. 于是由(3.11)，$T$ 关于 $\boldsymbol{B}'$的矩阵 A'的第一列将是$(c_1, 0, \cdots, 0)^t$，其中 c_1 是 v'_1 的特征值. 因此 A'具有

$$\left[\begin{array}{c|ccc} c_1 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right]$$

130

的形式，其中 B 是一个 $(n-1)\times(n-1)$ 矩阵．这一约化的矩阵版本是这样的：给定 $n\times n$ 矩阵 A，存在 $P\in GL_n(\mathbb{C})$，使得 $A'=PAP^{-1}$ 具有上面的形式．现在对 n 应用归纳法．由归纳法，我们可假设已证明存在某个 $Q\in GL_{n-1}(\mathbb{C})$，使得 QBQ^{-1} 是上三角的．设 Q_1 为 $n\times n$ 矩阵

$$\left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q & \\ 0 & & & \end{array}\right].$$

则

$$(Q_1P)A(Q_1P)^{-1}=Q_1(PAP^{-1})Q_1^{-1}=Q_1A'Q_1^{-1}$$

具有

$$\left[\begin{array}{c|ccc} c_1 & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & QBQ^{-1} & \\ 0 & & & \end{array}\right]$$

的形式，它是三角的． ■

我们已提到，证明的要点是每个复多项式有一个根．同样的证明对任意域 F 都可行，如果特征多项式所有的根都在域里．

【6.2】推论 设 F 为域．

(a) 向量空间形式：设 T 是域 F 上有限维向量空间 V 上的线性算子，且假设 T 的特征多项式在域 F 中分解为线性因子之积．则存在 V 的基 $\mathbf{B}$，使得 T 的矩阵 A 为上三角的．

(b) 矩阵形式：设 A 是 $n\times n$ 矩阵，其特征多项式在域 F 中分解为线性因子之积．则存在矩阵 $P\in GL_n(F)$，使得 PAP^{-1} 为上三角的．

证明 证明是相同的，除了在归纳步骤需要验证矩阵 B 的特征多项式为 $\dfrac{p(t)}{(t-c_1)}$，其中 $p(t)$ 是

131

A 的特征多项式．这是成立的，因为 $p(t)$ 也是 A' 的特征多项式，且 $\det(tI-A')=(t-c_1)\det(tI-B)$．这样我们对 A 的特征多项式分解为线性因子乘积的假设对于 B 也成立． ■

我们现在问哪些矩阵相似于对角矩阵．如(3.12)中所示，它们是以特征向量为基的矩阵 A．再设 $F=\mathbb{C}$，看一看特征多项式 $p(t)$ 的根．每一根都是某个特征向量的特征值，而每个特征向量只有一个特征值．大多数 n 次复多项式有 n 个不同的根，因而大多数复矩阵有 n 个特征值互不相同的特征向量，且假设特征向量可以构成一个基是合理的．这是正确的．

【6.3】命题 设 $v_1,\cdots,v_r\in V$ 为线性算子 T 的特征向量，具有不同的特征值 $c_1,\cdots,c_r$．则集合 $(v_1,\cdots,v_r)$ 线性无关．

证明 对 r 作数学归纳. 设给定相关关系

$$0=a_1v_1+\cdots+a_rv_r.$$

我们要证对所有 i 有 $a_i=0$，为此应用线性算子 T：

$$0=T(0)=a_1T(v_1)+\cdots+a_rT(v_r)=a_1c_1v_1+\cdots+a_rc_rv_r.$$

这是$(v_1,\cdots,v_r)$中的第二个相关关系. 我们从两个关系中消去 v_r，将第一个关系乘上 c_r 并减去第二个：

$$0=a_1(c_r-c_1)v_1+\cdots+a_{r-1}(c_r-c_{r-1})v_{r-1}.$$

应用归纳法原理，我们假设$(v_1,\cdots,v_{r-1})$是无关的. 于是系数 $a_1(c_r-c_1)$，…，$a_{r-1}(c_r-c_{r-1})$全为零. 因为 c_i 互不相同，若 $i<r$，则 $c_r-c_i\neq 0$. 这样 $a_1=\cdots=a_{r-1}=0$，而原来的关系化简为 $a_rv_r=0$. 因为特征向量不为零，亦有 $a_r=0$. ■

下面的定理由(3.12)和(6.3)合起来得到.

【6.4】定理 设 T 是域 F 上 n 维向量空间 V 的线性算子. 假定其特征多项式在 F 中有 n 个不同的根，则存在 V 的基使得 T 关于它的矩阵为对角形.

注意对角元素除了其顺序外是由线性算子 T 决定的. 它们是特征根.

当 $p(t)$有重根时，通常没有特征向量基，也难找到 T 的漂亮的矩阵. 研究这种情形可得出所谓的矩阵的若尔当标准形，我们将在第十二章加以讨论.

作为对角化的例子，考虑矩阵

$$A=\begin{bmatrix}3&2\\1&4\end{bmatrix},$$

132

其特征向量在(4.10)已计算出. 这些特征向量构成$\mathbb{R}^2$ 的基向量 $\boldsymbol{B}=(v_1,\ v_2)$. 根据第三章(4.20)[亦见注(5.24)]，联系标准基 $\boldsymbol{E}$ 与这个基 $\boldsymbol{B}$ 的矩阵为

【6.5】
$$P=[\boldsymbol{B}]^{-1}=\begin{bmatrix}1&2\\1&-1\end{bmatrix}^{-1}=-\frac{1}{3}\begin{bmatrix}-1&-2\\-1&1\end{bmatrix},$$

而 $PAP^{-1}=A'$为对角的：

【6.6】
$$-\frac{1}{3}\begin{bmatrix}-1&-2\\-1&1\end{bmatrix}\begin{bmatrix}3&2\\1&4\end{bmatrix}\begin{bmatrix}1&2\\1&-1\end{bmatrix}=\begin{bmatrix}5&\\&2\end{bmatrix}=A'.$$

一般规则在推论(6.7)中叙述：

【6.7】推论 若已知 A 在 F^n 中的一个特征向量的基 $\boldsymbol{B}$，并且 $P=[\boldsymbol{B}]^{-1}$，则 $A'=PAP^{-1}$ 为对角的.

定理(6.4)的重要性来自于用对角矩阵计算起来很容易这一事实. 例如，若 $A'=PAP^{-1}$ 为对角的，则矩阵 A 的幂可用公式

【6.8】
$$A^k=(P^{-1}A'P)^k=P^{-1}A'^kP$$

计算. 这样若 A 是矩阵(4.9)，则

$$\begin{aligned}A^k&=-\frac{1}{3}\begin{bmatrix}1&2\\1&-1\end{bmatrix}\begin{bmatrix}5&\\&2\end{bmatrix}^k\begin{bmatrix}-1&-2\\-1&1\end{bmatrix}\\&=\frac{1}{3}\begin{bmatrix}5^k+2\cdot 2^k&2(5^k-2^k)\\5^k-2^k&2\cdot 5^k+2^k\end{bmatrix}.\end{aligned}$$

第七节 微分方程组

在微积分中我们学过一阶线性微分方程

【7.1】
$$\frac{dx}{dt}=ax$$

的解为 $x(t)=ce^{at}$，其中 c 为任意常数. 显然，ce^{at} 是方程(7.1)的解. 要证每一个解都有这样的形式，设可微函数 $x(t)$ 是一个解. 利用乘积法则求微分 $e^{-at}x(t)$：

$$\frac{d}{dt}(e^{-at}x(t))=-ae^{-at}x(t)+e^{-at}ax(t)=0.$$

这样 $e^{-at}x(t)$ 是常数 c，于是 $x(t)=ce^{at}$.

作为对角化的一个应用，我们将这个解拓广到微分方程组. 为了用矩阵记号写出方程，我们使用下面的术语. 一个向量值函数 $X(t)$ 是元素为 t 的函数的向量. 类似地，一个矩阵值函数 $A(t)$ 是元素为函数的矩阵：

133

【7.2】
$$X(t)=\begin{bmatrix}x_1(t)\\ \vdots\\ x_n(t)\end{bmatrix},\quad A(t)=\begin{bmatrix}a_{11}(t) & \cdots & a_{1n}(t)\\ \vdots & \cdots & \vdots\\ a_{m1}(t) & \cdots & a_{mn}(t)\end{bmatrix}.$$

取极限、微分等微积分运算，通过分别对每一个元素进行运算也拓广到向量值和矩阵值函数. 这样由定义有

【7.3】
$$\lim_{t\to t_0}X(t)=\begin{bmatrix}\xi_1\\ \vdots\\ \xi_n\end{bmatrix},\quad 其中\ \xi_i=\lim_{t\to t_0}x_i(t).$$

因此这个极限存在当且仅当对每一个 i，$\lim_{t\to t_0}x_i(t)$ 存在. 同样地，向量值或矩阵值函数的导数是分别对每个元素求导得到的函数：

$$\frac{dX}{dt}=\begin{bmatrix}x'_1(t)\\ \vdots\\ x'_n(t)\end{bmatrix},\quad \frac{dA}{dt}=\begin{bmatrix}a'_{11}(t) & \cdots & a'_{1n}(t)\\ \vdots & & \vdots\\ a'_{m1}(t) & \cdots & a'_{mn}(t)\end{bmatrix},$$

其中 $x'_i(t)$ 是 $x_i(t)$ 的导数，等等. 因而 $\frac{dX}{dt}$ 有定义当且仅当每一个函数 $x_i(t)$ 可微. 导数也可用向量符号描述为

【7.4】
$$\frac{dX}{dt}=\lim_{h\to 0}\frac{X(t+h)-X(t)}{h}.$$

其中 $X(t+h)-X(t)$ 用向量加法计算，分母上的 h 是指用 h^{-1} 乘的标量. 极限是如上所示的分别在每个元素上取极限. 因而(7.4)的元素为导数 $x'_i(t)$. 对矩阵值函数同样的结论也是正确的.

齐次一阶线性常系数微分方程组是形如

【7.5】
$$\frac{dX}{dt}=AX$$

的矩阵方程，其中 A 是一个 $n\times n$ 实的或复的矩阵而 $X(t)$ 为 n 维向量值函数．写出这样的方程组，我们得到形如

134

【7.6】
$$\begin{aligned}\frac{\mathrm{d}x_1}{\mathrm{d}t} &= a_{11}x_1(t)+\cdots+a_{1n}x_n(t)\\ &\vdots\\ \frac{\mathrm{d}x_n}{\mathrm{d}t} &= a_{n1}x_1(t)+\cdots+a_{nn}x_n(t)\end{aligned}$$

的 n 个微分方程的方程组．$x_i(t)$ 是未知函数，a_{ij} 是标量．例如，若用矩阵 $\begin{bmatrix}3 & 2\\ 1 & 4\end{bmatrix}$ 代替 A，(7.5)便成为两个未知量的两个方程的方程组：

【7.7】
$$\begin{aligned}\frac{\mathrm{d}x_1}{\mathrm{d}t} &= 3x_1+2x_2\\ \frac{\mathrm{d}x_2}{\mathrm{d}t} &= x_1+4x_2.\end{aligned}$$

最简单的方程组(7.5)是其中的 A 为对角矩阵的那些．设对角元素为 a_i，则方程(7.6)写成

【7.8】
$$\frac{\mathrm{d}x_i}{\mathrm{d}t}=a_ix_i(t),\quad i=1,\cdots,n.$$

这里未知函数 x_i 没有被方程混合起来，因而对某个常数 c_i 我们可以分别解出每一个

【7.9】
$$x_i=c_i\mathrm{e}^{a_it}.$$

可以在大多数情形下解方程(7.5)的事实是：若 v 是 A 的一个特征值为 a 的特征向量，则

【7.10】
$$X=\mathrm{e}^{at}v$$

是(7.5)的一个特解．这里 $\mathrm{e}^{at}v$ 解释为函数 e^{at} 与向量 v 的标量积．微分作用于标量函数，固定常向量 v，而用 A 左乘作用于向量 v，固定标量函数 e^{at}．这样 $\frac{\mathrm{d}}{\mathrm{d}t}\mathrm{e}^{at}v=a\,\mathrm{e}^{at}v=A\mathrm{e}^{at}v$．例如，$(2,-1)^t$ 是矩阵 $\begin{bmatrix}3 & 2\\ 1 & 4\end{bmatrix}$ 的特征向量，其特征值为 2，$\begin{bmatrix}2\mathrm{e}^{2t}\\ -\mathrm{e}^{2t}\end{bmatrix}$ 是微分方程组(7.7)的解．

这一事实使我们能够在矩阵 A 有不同的实特征值时解方程组(7.5)．在这一情形中，每一解将是特解(7.10)的线性组合．通过对角化可方便地将解求出来．这里用～代替上一节使用的记号′，以避免与微分混淆．设 P 为使 $PAP^{-1}=\widetilde{A}$ 为对角的可逆矩阵．于是 $P=[\boldsymbol{B}]^{-1}$，其中 $\boldsymbol{B}$ 是特征向量的一个基．作变量的线性变换

135

【7.11】
$$X=P^{-1}\widetilde{X}.$$

于是

【7.12】
$$\frac{\mathrm{d}X}{\mathrm{d}t}=P^{-1}\frac{\mathrm{d}\widetilde{X}}{\mathrm{d}t}.$$

代入(7.5)，得到

【7.13】
$$\frac{\mathrm{d}\widetilde{X}}{\mathrm{d}t}=PAP^{-1}\widetilde{X}=\widetilde{A}\widetilde{X}.$$

因为$\widetilde{A}$是对角的，变量$\widetilde{x}_i$被分离开来，故方程可用指数函数求解. $\widetilde{A}$的对角元是A的特征值λ_1，…，λ_n，因而方程组(7.13)的解为

【7.14】 $$\widetilde{x}_i = c_i e^{\lambda_i t}, \quad \text{对某个 } c_i \text{ 成立.}$$

代回去，得

【7.15】 $$X = P^{-1}\widetilde{X}$$

是原方程(7.5)的解. 这证明了下面的命题：

【7.16】命题 设A是$n\times n$矩阵，P是可逆矩阵且$PAP^{-1}=\widetilde{A}$是对角的，对角元为λ_1，…，λ_n. 方程组$\frac{dX}{dt}=AX$的一般解是$X=P^{-1}\widetilde{X}$，其中$\widetilde{x}_i=c_ie^{\lambda_i t}$，$c_i$是任意常数.

例(7.7)中对角化A的矩阵已在(6.5)中算出：

【7.17】 $$P^{-1}=\begin{bmatrix}1 & 2\\ 1 & -1\end{bmatrix},\quad \widetilde{A}=\begin{bmatrix}5 & \\ & 2\end{bmatrix}.$$

这样

$$\begin{bmatrix}\widetilde{x}_1\\ \widetilde{x}_2\end{bmatrix}=\begin{bmatrix}c_1e^{5t}\\ c_2e^{2t}\end{bmatrix},$$

【7.18】 $$\begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}1 & 2\\ 1 & -1\end{bmatrix}\begin{bmatrix}c_1e^{5t}\\ c_2e^{2t}\end{bmatrix}=\begin{bmatrix}c_1e^{5t}+2c_2e^{2t}\\ c_1e^{5t}-c_2e^{2t}\end{bmatrix}.$$

换言之，每个解为两个基本解

136

$$\begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}e^{5t}\\ e^{5t}\end{bmatrix} \quad \text{和} \quad \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}2e^{2t}\\ -e^{2t}\end{bmatrix}$$

的线性组合. 它们是对应于特征向量$(1, 1)^t$和$(2, -1)^t$的解(7.10). 这些解中出现的系数c_i是任意的. 它们通常由指定的*初始条件*，即X在某特殊t_0的值决定.

我们现在考虑系数矩阵A有不同的特征值、但是不全为实数的情形. 为了重复我们上面所用的方法，必须先考虑形如(7.1)的微分方程，其中a为复数. 通过适当的解释，这样的微分方程的解仍为ce^{at}的形式. 我们要记住的是e^{at}现在是t的复值函数. 为集中我们的注意力，在这里将变量t限制为实数值，虽然在做复值函数时这并不是最自然的选择. 允许t取复值将不会有太大的变化.

复值函数导数的定义与实值函数是一样的：

【7.19】 $$\frac{dx}{dt}=\lim_{h\to 0}\frac{x(t+h)-x(t)}{h},$$

如果这个极限存在. 不会出现新的特性. 可将这样的函数$x(t)$用实值函数，即其实部和虚部写出来：

【7.20】 $$x(t)=u(t)+iv(t).$$

则x是可微的当且仅当u和v都是可微的，且当它们可微时，x的导数为$x'=u'+iv'$. 这由定义就可直接得到. 通常的微分法则(比如乘积法则)对复值函数成立. 这些法则可在u和v上应用实函数相应的定理得到，也可将实函数的证明搬到复函数的情形.

回忆公式

【7.21】
$$e^{r+si}=e^{r}(\cos s+i\sin s).$$

这个公式的微分表明对所有复数 $a=r+si$，$\frac{de^{at}}{dt}=ae^{at}$ 成立．因此 ce^{at} 是方程(7.1)的解，本节开头的证明表明这是仅有的解．

将一个方程的情形拓广到了复系数的情形后，当 A 是具有不同特征值的任意复矩阵时，可以用对角化方法解方程组(7.5)．

例如，设 $A=\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix}$．向量 $v_1=\begin{bmatrix}1\\ i\end{bmatrix}$ 和 $v_2=\begin{bmatrix}i\\ 1\end{bmatrix}$ 分别是特征值为 $1+i$ 和 $1-i$ 的特征向量．设 $\boldsymbol{B}=(v_1,\ v_2)$．根据(6.7)，$A$ 可以由矩阵 P 对角化，其中

【7.22】
$$P^{-1}=[\boldsymbol{B}]=\begin{bmatrix}1 & i\\ i & 1\end{bmatrix}.$$

137

公式(7.14)告诉我们 $\widetilde{X}=\begin{bmatrix}\widetilde{x}_1\\ \widetilde{x}_2\end{bmatrix}=\begin{bmatrix}c_1e^{t+it}\\ c_2e^{t-it}\end{bmatrix}$．(7.5)的解是

【7.23】
$$\begin{bmatrix}x_1\\ x_2\end{bmatrix}=P^{-1}\widetilde{X}=\begin{bmatrix}c_1e^{t+it}+ic_2e^{t-it}\\ ic_1e^{t+it}+c_2e^{t-it}\end{bmatrix},$$

其中 c_1，c_2 是任意复数．因而每个解都是两个基本解

【7.24】
$$\begin{bmatrix}e^{t+it}\\ ie^{t+it}\end{bmatrix}\quad 和\quad \begin{bmatrix}ie^{t-it}\\ e^{t-it}\end{bmatrix}$$

的线性组合．然而，这些解并不是完全令人满意的，因为我们从实系数微分方程开始，得到的答案却是复的．当原来的矩阵为实的，我们想要的解为实解．我们注意下面的引理：

【7.25】引理 *设 A 是实 $n\times n$ 矩阵，并设 $X(t)$ 为微分方程(7.5)的复值解．则 $X(t)$ 的实部和虚部也是同一方程的解．*

现在原方程(7.5)的每个解无论是实的还是复的，对某个复数 c_i 都具有(7.23)的形式．因而实解亦在我们所得的解之中．为了把它们具体写出，可取复解的实部和虚部．

基本解(7.24)的实部和虚部由等式(7.21)确定．它们为

【7.26】
$$\begin{bmatrix}e^{t}\cos t\\ -e^{t}\sin t\end{bmatrix}\quad 和\quad \begin{bmatrix}e^{t}\sin t\\ e^{t}\cos t\end{bmatrix}.$$

每个实解都是这些特解的实线性组合．

第八节　矩阵指数

一阶线性常系数微分方程组亦可用矩阵指数形式求解．$n\times n$ 实或复矩阵 A 的指数由将矩阵代入 e^{x} 的泰勒展开式

【8.1】
$$1+\frac{x}{1!}+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots$$

得到．这样由定义，

【8.2】
$$e^A = I + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \cdots.$$

138 这是一个 $n\times n$ 矩阵.

【8.3】命题　级数(8.2)对所有复矩阵 A 绝对收敛.

为了不使讨论被打断，我们将证明集中放在本节结尾处.

因为矩阵乘法相对较为复杂，直接写出 e^A 的矩阵元素并不容易. 特别是 e^A 的元素通常不是由 A 的元素取幂得到. 但在一种情形下这是可能的，此时指数很容易计算，这就是当 A 是对角矩阵时，假设其对角元素为 a_i. 考察该级数表明 e^A 亦为对角的，并且此时对角元素为 e^{a_i}.

对于 2×2 三角矩阵，指数的计算也相对比较容易. 例如，设

【8.4】
$$A = \begin{bmatrix} 1 & 1 \\ & 2 \end{bmatrix}.$$

则

【8.5】
$$e^A = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ & 2 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 & 3 \\ & 4 \end{bmatrix} + \cdots = \begin{bmatrix} e & * \\ & e^2 \end{bmatrix}.$$

对角元素取幂得到 e^A 的对角元. 可由定义直接算出缺失的元素 *.

只要知道有矩阵 P 使 PAP^{-1} 是对角的，就可以确定矩阵 A 的指数. 应用法则 $PA^kP^{-1} = (PAP^{-1})^k$ 和矩阵乘法的分配律，我们得到

【8.6】
$$Pe^AP^{-1} = PIP^{-1} + (PAP^{-1}) + \frac{1}{2!}(PAP^{-1})^2 + \cdots = e^{PAP^{-1}}.$$

设 $PAP^{-1} = \widetilde{A}$ 是对角的，对角元素为 λ_i. 则 $e^{\widetilde{A}}$ 也是对角的，其对角元素为 e^{λ_i}. 因此可以具体地算出 e^A：

【8.7】
$$e^A = P^{-1}e^{\widetilde{A}}P.$$

为了使用矩阵指数解微分方程组，我们需要将普通指数的一些性质延拓到矩阵指数. 最基本的性质是 $e^{x+y} = e^xe^y$. 这一性质由展开

【8.8】
$$e^{x+y} = 1 + \frac{(x+y)}{1!} + \frac{(x+y)^2}{2!} + \cdots \quad \text{和}$$
$$e^xe^y = \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots\right)\left(1 + \frac{y}{1!} + \frac{y^2}{2!} + \cdots\right)$$

得到的两个无穷级数的形式恒等式表示. 因为两个级数的相等需要用到交换律，我们不能把矩阵代入这个等式. 例如，当交换律不成立时，计算(8.8)的二次项分别得到 $\frac{1}{2}(x^2 + xy + yx +$ 139 $y^2)$ 和 $\frac{1}{2}x^2 + xy + \frac{1}{2}y^2$. 除非 $xy = yx$，否则它们是不相等的. 因而，没有理由期望 e^{A+B} 和 e^Ae^B 通常是相等的. 然而，如果两个矩阵 A 和 B 是可交换的，则可以应用形式恒等式.

【8.9】命题

1. 对于交换的变量 x，y，形式展开式(8.8)相等.

2. 设 A，B 是交换的复 $n\times n$ 矩阵：$AB=BA$. 则有 $e^{A+B}=e^{A}e^{B}$.

证明见本节结尾.

【8.10】推论 对任意复 $n\times n$ 矩阵 A，指数 e^{A} 是可逆的，其逆为 e^{-A}.

这可由命题得到，因为 A 与 $-A$ 可交换，所以 $e^{A}e^{-A}=e^{A-A}=e^{0}=I$.

作为命题(8.9b)的一个应用，考虑矩阵

【8.11】
$$A=\begin{bmatrix}2 & 3\\ & 2\end{bmatrix}.$$

将它写为 $A=2I+B$ 的形式，其中 $B=3e_{12}$，我们可计算其指数. 因为 $2I$ 与 B 可交换，应用命题(8.9b)得：$e^{A}=e^{2I}e^{B}$，由级数展开可以得到 $e^{2I}=e^{2}I$ 和 $e^{B}=I+B$. 于是

$$e^{A}=\begin{bmatrix}e^{2} & \\ & e^{2}\end{bmatrix}\begin{bmatrix}1 & 3\\ & 1\end{bmatrix}=\begin{bmatrix}e^{2} & 3e^{2}\\ & e^{2}\end{bmatrix}.$$

我们现在可以得到联系矩阵指数与微分方程的主要定理. 给定 $n\times n$ 矩阵 A，我们考虑指数 e^{tA}（其中 t 是一标量变量）作为矩阵值函数：

【8.12】
$$e^{tA}=I+tA+\frac{t^{2}}{2!}A^{2}+\frac{t^{3}}{3!}A^{3}+\cdots.$$

【8.13】命题 e^{tA} 是 t 的一个可微函数，其导数为 Ae^{tA}.

证明见本节结尾.

【8.14】定理 设 A 为实或复 $n\times n$ 矩阵. 矩阵 e^{tA} 的列构成微分方程

$$\frac{dX}{dt}=AX$$

的解的向量空间的基.

我们将需要下面的引理，其证明留作练习.

140

【8.15】引理 乘积法则：设 $A(t)$ 和 $B(t)$ 是 t 的两个可微矩阵值函数，其行列数适当使乘积有定义. 则矩阵乘积 $A(t)B(t)$ 可微，且其导数为

$$\frac{d}{dt}(A(t)B(t))=\frac{dA}{dt}B+A\frac{dB}{dt}.$$

定理(8.14)的证明 命题(8.13)表明 A 的列是微分方程的解，因为微分与 A 的乘积在矩阵 e^{tA} 的列上的作用是独立的. 要证每个解是列的线性组合，我们只需复制第七节开始给出的证明. 设 $X(t)$ 是(7.5)的任意一个解. 对矩阵乘积 $e^{-tA}X(t)$ 求微分，得

$$\frac{d}{dt}(e^{-tA}X(t))=-Ae^{-tA}X(t)+e^{-tA}AX(t).$$

幸运的是，A 与 e^{-tA} 可交换. 这可直接由指数的定义得到. 所以导数为零. 由此得 $e^{-tA}X(t)$ 是一个常列向量，比如设为 $C=(c_{1},\cdots,c_{n})^{t}$，则 $X(t)=e^{tA}C$. 这就把 $X(t)$ 表示为 e^{tA} 列向量的线性组合. 由于 e^{tA} 是可逆矩阵，这个表达式是唯一的. ■

根据定理(8.14)，矩阵指数总是微分方程(7.5)的解. 因为指数的直接计算非常困难，所以这个定理在具体情形的应用并不容易. 但如果 A 是可对角化的矩阵，则指数可用(8.7)计算：$e^{A}=P^{-1}e^{\widetilde{A}}P$. 我们可用计算 e^{tA} 的方法解方程(7.5)，当然得到与前面相同的结果. 这样，

如果 A 是例(7.7)中所用的矩阵，P，$\widetilde{A}$ 如(7.17)给出，则

$$e^{t\widetilde{A}}=\begin{bmatrix}e^{5t} & \\ & e^{2t}\end{bmatrix},$$

而

$$e^{tA}=P^{-1}e^{t\widetilde{A}}P=-\frac{1}{3}\begin{bmatrix}1 & 2\\ 1 & -1\end{bmatrix}\begin{bmatrix}e^{5t} & \\ & e^{2t}\end{bmatrix}\begin{bmatrix}-1 & -2\\ -1 & 1\end{bmatrix}$$

$$=\frac{1}{3}\begin{bmatrix}e^{5t}+2e^{2t} & 2e^{5t}-2e^{2t}\\ e^{5t}-e^{2t} & 2e^{5t}+e^{2t}\end{bmatrix}.$$

我们得到的列构成(7.18)一般解的第二个基.

另一方面，矩阵 $A=\begin{bmatrix}1 & \\ 1 & 1\end{bmatrix}$ 表示方程组

【8.16】 $$\frac{dx}{dt}=x,\quad \frac{dy}{dt}=x+y,$$

141

它是不可对角化的. 因此第七节的方法不能用. 为解这个方程组，我们将 At 写为 $At=It+Bt$，其中 $B=e_{21}$，并用与(8.11)同样的讨论得到

【8.17】 $$e^{At}=e^{It}e^{Bt}=\begin{bmatrix}e^{t} & \\ te^{t} & e^{t}\end{bmatrix}.$$

这样(8.16)的解是列向量

【8.18】 $$\begin{bmatrix}e^{t}\\ te^{t}\end{bmatrix},\quad \begin{bmatrix}0\\ e^{t}\end{bmatrix}$$

的线性组合. 要对所有情形具体算出矩阵指数，需要将矩阵化为若尔当标准形(见第十二章).

现在我们回到命题(8.3)、(8.9)和(8.13)的证明. 为了使得记号更为紧凑，我们将矩阵 A 的 i，j-元素记为 A_{ij}. 这样，$(AB)_{ij}$ 将表示乘积矩阵 AB 的元素，而 $(A^k)_{ij}$ 表示 A^k 的元素. 借助这个记号，e^A 的 i，j-元素是级数

【8.19】 $$(e^A)_{ij}=I_{ij}+A_{ij}+\frac{1}{2!}(A^2)_{ij}+\frac{1}{3!}(A^3)_{ij}+\cdots.$$

为了证明指数级数收敛，我们需要证明给定矩阵的幂 A^k 的元素不会增长得太快，从而其 i，j-元素的绝对值构成一个有界(因而收敛)的级数. 将 $n\times n$ 矩阵 A 的范数定义为矩阵元素最大的绝对值：

【8.20】 $$\|A\|=\max_{i,j}|A_{ij}|.$$

换言之，$\|A\|$ 是满足

【8.21】 $$对所有\ i,j\ 有\ |A_{ij}|\leqslant\|A\|$$

的最小实数. 这是范数的几种可能的定义之一. 其基本性质如下：

【8.22】引理 设 A，B 是复 $n\times n$ 矩阵. 则 $\|AB\|\leqslant n\|A\|\|B\|$，且对所有 $k>0$ 有 $\|A^k\|\leqslant n^{k-1}\|A\|^k$.

证明 我们估计 AB 的 i，j-元素的大小：

$$|(AB)_{ij}|=\left|\sum_{\nu}A_{i\nu}B_{\nu j}\right|\leqslant\sum_{\nu=1}^{n}|A_{i\nu}||B_{\nu j}|\leqslant n\|A\|\|B\|.$$

这样 $\|AB\|\leqslant n\|A\|\|B\|$. 从第一个不等式出发，作数学归纳法可得第二个不等式. ■

命题(8.3)的证明 为证矩阵指数绝对收敛，我们对级数作如下估计：设 $a=n\|A\|$. 则 142

【8.23】

$$\begin{aligned}|(e^{A})_{ij}|&\leqslant|I_{ij}|+|A_{ij}|+\frac{1}{2!}|(A^2)_{ij}|+\frac{1}{3!}|(A^3)_{ij}|+\cdots\\&\leqslant1+\|A\|+\frac{1}{2!}n\|A\|^2+\frac{1}{3!}n^2\|A\|^3+\cdots\\&=1+\frac{\left(a+\frac{1}{2!}a^2+\frac{1}{3!}a^3+\cdots\right)}{n}=1+\frac{e^a-1}{n}.\end{aligned}$$ ■

命题(8.9)的证明

(a) 展开式(8.8)的 k 次项是

$$(x+y)^k/k!=\sum_{r+s=k}\binom{k}{r}x^ry^s/k!\quad 和\quad \sum_{r+s=k}\frac{x^ry^s}{r!s!}.$$

为证这两项相等，需证

$$\binom{k}{r}/k!=\frac{1}{r!s!}\quad 或\quad \binom{k}{r}=\frac{k!}{r!s!}$$

对满足 $r+s=k$ 的所有 k 及所有 r，s 成立. 这是二项式系数的标准公式.

(b) 用 $S_n(x)$ 表示部分和 $1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots\frac{x^n}{n!}$. 则

$$\begin{aligned}S_n(x)S_n(y)&=\left(1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}\right)\left(1+\frac{y}{1!}+\frac{y^2}{2!}+\cdots+\frac{y^n}{n!}\right)\\&=\sum_{r,s=0}^{n}\frac{x^ry^s}{r!s!},\end{aligned}$$

而

$$S_n(x+y)=\left(1+\frac{(x+y)}{1!}+\frac{(x+y)^2}{2!}+\cdots+\frac{(x+y)^n}{n!}\right)$$

$$=\sum_{k=0}^{n}\sum_{r+s=k}\binom{k}{r}x^ry^s/k!=\sum_{k=0}^{n}\sum_{r+s=k}\frac{x^ry^s}{r!s!}.$$

比较各项，我们发现部分和 $S_n(x+y)$ 的展示由 $S_n(x)S_n(y)$ 中满足 $r+s\leqslant n$ 的项组成. 当用 A，B 替代 x，y 时同样成立. 我们需证当 $k\longrightarrow\infty$ 时，余项之和趋于零.

【8.24】引理 对所有 i,j，级数 $\sum\limits_{k}\sum\limits_{r+s=k}\left|\left(\frac{A^r}{r!}\frac{B^s}{s!}\right)_{ij}\right|$ 收敛.

证明 设 $a=n\|A\|$ 和 $b=n\|B\|$. 我们估计和中的项. 根据(8.22)，$|(A^rB^s)_{ij}|\leqslant n(n^{r-1}\|A\|^r)(n^{s-1}\|B\|^s)\leqslant a^rb^s$. 于是

$$\sum_{k}\sum_{r+s=k}\left|\left(\frac{A^r}{r!}\frac{B^s}{s!}\right)_{ij}\right|\leqslant\sum_{k}\sum_{r+s=k}\frac{a^r}{r!}\frac{b^s}{s!}=e^{a+b}.$$

143

命题由这个引理得到，因为一方面 i，j-元素

$$(S_k(A)S_k(B)-S_k(A+B))_{ij}\text{ 有上界}\sum_{r+s>k}\left|\left(\frac{A^r}{r!}\frac{B^s}{s!}\right)_{ij}\right|.$$

根据引理，当 $k\longrightarrow\infty$ 时，这个和趋于零．而另一方面

$$(S_k(A)S_k(B)-S_k(A+B))\longrightarrow(e^Ae^B-e^{A+B}).$$

■

命题(8.13)的证明 由定义，

$$\frac{d}{dt}(e^{tA})=\lim_{h\to 0}\frac{e^{(t+h)A}-e^{tA}}{h}.$$

因为矩阵 tA 与 hA 可交换，命题(8.9)表明

$$\frac{e^{(t+h)A}-e^{tA}}{h}=\left(\frac{e^{hA}-I}{h}\right)e^{tA}.$$

因此，我们的命题由下面引理得到：

【8.25】引理 $\lim\limits_{h\to 0}\dfrac{e^{hA}-I}{h}=A.$

证明 指数的级数展开给出

【8.26】

$$\frac{e^{hA}-I}{h}-A=\frac{h}{2!}A^2+\frac{h^2}{3!}A^3+\cdots.$$

我们估计这个级数：设 $a=|h|n\|A\|$．则

$$\begin{aligned}\left|\left(\frac{h}{2!}A^2+\frac{h^2}{3!}A^3+\cdots\right)_{ij}\right| &\leqslant\left|\frac{h}{2!}(A^2)_{ij}\right|+\left|\frac{h^2}{3!}(A^3)_{ij}\right|+\cdots\\ &\leqslant\frac{1}{2!}|h|n\|A\|^2+\frac{1}{3!}|h|^2n^2\|A\|^3+\cdots\\ &=\|A\|\left(\frac{1}{2!}a+\frac{1}{3!}a^2+\cdots\right)\\ &=\frac{\|A\|}{a}(e^a-1-a)=\|A\|\left(\frac{e^a-1}{a}-1\right).\end{aligned}$$

注意当 $h\longrightarrow 0$ 时 $a\longrightarrow 0$．因为 e^x 的导数为 e^x，

$$\lim_{a\longrightarrow 0}\frac{e^a-1}{a}=\frac{d}{dx}e^x\bigg|_{x=0}=e^0=1.$$

于是(8.26)随 h 趋于零． ■

144 在第八章，我们还会用到矩阵指数这些非同寻常的性质．

我从未想过有必要费力对定理的

一般情形给出形式的证明．

Arthur Cayley

练 习

第一节 维数公式

1. 设 T 是矩阵 $\begin{bmatrix}1&2&0&-1&5\\2&0&2&0&1\\1&1&-1&3&2\\0&3&-3&2&6\end{bmatrix}$ 的左乘．通过给出它们的基，具体计算 $\ker T$ 和 $\operatorname{im}T$，验证(1.7)．

2. 求矩阵$\begin{bmatrix}11 & 12 & 13 & 14\\21 & 22 & 23 & 24\\31 & 32 & 33 & 34\\41 & 42 & 43 & 44\end{bmatrix}$的秩.

3. 设 $T: V \longrightarrow W$ 是线性变换．证明 $\ker T$ 是 V 的子空间而 $\operatorname{im} T$ 是 W 的子空间.

4. 设 A 是 $m\times n$ 阶矩阵．证明线性方程组 $AX=0$ 的解空间的维数至少是 $n-m$.

5. 设 A 是 $k\times m$ 阶矩阵并设 B 是 $n\times p$ 阶矩阵．证明法则 $M \rightsquigarrow AMB$ 定义一个由 $m\times n$ 阶矩阵空间 $F^{m\times n}$ 到空间 $F^{k\times p}$ 的线性变换.

6. 设$(v_1, \cdots, v_n)$是向量空间 V 的子集．证明由 $\varphi(X)=v_1x_1+\cdots+v_nx_n$ 定义的映射$\varphi: F^n \longrightarrow V$ 是一个线性变换.

7. 当域为域$\mathbb{F}_p$ 中的一个时，有限维向量空间有有限多个元素．在这种情形中公式(1.6)和第二章公式(6.15)都可用．比较它们.

8. 证明每一个秩为 1 的 $m\times n$ 矩阵具有 $A=XY^t$ 的形式，其中 X，Y 为 m-维和 n-维列向量.

9. (a) $V=\mathbb{R}^\infty$ 上的*左移位算子* S^- 由$(a_1, a_2, \cdots) \rightsquigarrow (a_2, a_3, \cdots)$定义．证明 $\ker S^- > 0$ 且 $\operatorname{im} S^- = V$.

   (b) $V=\mathbb{R}^\infty$ 上的*右移位算子* S^+ 由$(a_1, a_2, \cdots) \rightsquigarrow (0, a_1, a_2, \cdots)$定义．证明 $\ker S^+ = 0$ 且 $\operatorname{im} S^+ < V$.

第二节 线性变换的矩阵

1. 确定微分算子$\frac{d}{dx}$：$P_n \longrightarrow P_{n-1}$关于自然基(见(1.4))的矩阵.

2. 求将直线 $y=x$ 变到直线 $y=3x$ 的线性变换 $T: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$.

3. 用行和列变换证明命题(2.9b).

145

4. 设 $T: \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ 是由规则 $T(x_1, x_2, x_3)^t=(x_1+x_2, 2x_3-x_1)^t$ 定义的线性变换．T 关于标准基的矩阵是什么?

5. 设 A 是 $n\times n$ 矩阵，且设 $V=F^n$ 表示行向量空间．线性算子"用 A 右乘"关于 V 的标准基的矩阵是什么?

6. 证明不同的矩阵定义不同的线性变换.

7. 描述矩阵(2.10)的左乘和右乘，并证明该矩阵的秩为 r.

8. 证明矩阵 A 与 A^t 有相同的秩.

9. 设 T_1，T_2 是从 V 到 W 的线性变换．用规则$[T_1+T_2](v)=T_1(v)+T_2(v)$和$[cT](v)=cT(v)$定义 T_1+T_2 和 cT.

   (a) 证明 T_1+T_2 和 cT 是线性变换，并用 T_1 和 T_2 的矩阵描述它们的矩阵.

   (b) 设 L 是 V 到 W 的全体线性变换的集合．证明这些法则使 L 成为向量空间，并求其维数.

第三节 线性算子和特征向量

1. 设 V 是实 2×2 对称矩阵 $X=\begin{bmatrix}x & y\\y & z\end{bmatrix}$的向量空间，并设 $A=\begin{bmatrix}2 & 1\\ & 1\end{bmatrix}$. 确定在 V 上由 $X \rightsquigarrow AXA^t$ 定义的线性算子关于适当的基的矩阵.

2. 设 $A=(a_{ij})$，$B=(b_{ij})$为 2×2 矩阵，考虑 2×2 矩阵空间 $F^{2\times 2}$ 上的线性算子 $T: M \rightsquigarrow AMB$. 求 T 关于 $F^{2\times 2}$ 的基$(e_{11}, e_{12}, e_{21}, e_{22})$的矩阵.

3. 设 $T: V \longrightarrow V$ 是 2 维向量空间的线性算子．设 T 不是用标量乘．证明存在向量 $v\in V$ 使得$(v, T(v))$是 V 的基，并描述 T 关于这个基的矩阵.

4. 设 T 是向量空间 V 的线性算子，并设 $c\in F$. 设 W 是具有特征值 c 的特征向量加上 0 的集合．证明 W 是一个 T-不变子空间.

5. 求矩阵为(a)$\begin{bmatrix}1 & 1\\ & 1\end{bmatrix}$和(b)$\begin{bmatrix}1 & & \\ & 2 & \\ & & 3\end{bmatrix}$的实线性算子的所有不变子空间.

6. 向量空间 V 的一个算子称为幂零的，如果存在某个 k 使得 $T^k=0$. 设 T 是幂零算子且设 $W^i=\mathrm{im}T^i$.

(a) 证明若 $W^i\neq 0$，则 $\dim W^{i+1}<\dim W^i$.

(b) 证明如果 V 是 n 维向量空间且如果 T 是幂零的，则 $T^n=0$.

7. 设 T 是$\mathbb{R}^2$ 上的线性算子. 证明如果 T 将直线 ℓ 映到 ℓ，则它亦将每一条与 ℓ 平行的直线映为另一条与 ℓ 平行的直线.

8. 证明向量空间的线性算子的合成 $T_1\circ T_2$ 是一个线性算子，并用 T_1，T_2 的矩阵 A_1，A_2 计算其矩阵.

146

9. 设 P 是次数$\leqslant n$ 的多项式 $p(x)=a_0+a_1x+\cdots+a_nx^n$ 的实空间，设 D 表示导数$\dfrac{\mathrm{d}}{\mathrm{d}x}$，把它视为 P 上的线性算子.

(a) 求 D 关于一个方便的基的矩阵，并证明 D 是幂零算子.

(b) 求所有 D-不变子空间.

10. 证明矩阵$\begin{bmatrix}a & 0\\ 0 & d\end{bmatrix}$与$\begin{bmatrix}a & b\\ 0 & d\end{bmatrix}$相似当且仅当 $a\neq d$.

11. 设 $A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$是实 2×2 矩阵. 证明除了 $b=c=0$ 且 $a=d$ 的情形外，A 可通过形如 $A\longrightarrow EAE^{-1}$ 的初等行列变换约简为矩阵$\begin{bmatrix}0 & *\\ 1 & *\end{bmatrix}$. 仔细分析 b 或 c 为 0 的可能情形.

12. 设 T 是$\mathbb{R}^2$ 上的有两个线性无关特征向量 v_1，v_2 的线性算子. 假设这些算子的特征值 c_1，c_2 是正的且 $c_1>c_2$. 设 ℓ_i 是 v_i 张成的直线.

(a) 算子 T 将每条过原点的直线 ℓ 变到另一条直线. 利用向量加法的平行四边形法则，证明每条直线 $\ell\neq\ell_2$ 被从 ℓ_2 平移到 ℓ_1.

(b) 用(a)证明仅有的特征向量是 v_1 或 v_2 的倍数.

(c) 当只有一条直线被映到自身且有正特征值时，描述对直线作用的效果.

13. 考虑任意一个 2×2 矩阵 $A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$. 列向量 X 是用 A 左乘的特征向量的条件是 $Y=AX$ 与 X 平行，这表明斜率 $s=\dfrac{x_2}{x_1}$ 与 $s'=\dfrac{y_2}{y_1}$ 相等.

(a) 求 s 中表示这一等式的方程.

(b) $s=0$ 是哪些 A 的解，$s=\infty$ 呢?

(c) 证明如果 A 的元素是正实数，则在第一象限有一个特征向量，在第二象限也有一个特征向量.

第四节　特征多项式

1. 对下列复矩阵求特征多项式、特征值和特征向量.

(a) $\begin{bmatrix}-2 & 2\\ -2 & 3\end{bmatrix}$　(b) $\begin{bmatrix}1 & \mathrm{i}\\ -\mathrm{i} & 1\end{bmatrix}$

2. (a) 证明实对称 2×2 矩阵特征值是实数.

(b) 证明非对角元为正的实 2×2 矩阵有实的特征值.

3. 求旋转矩阵$\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}$的复特征值和特征向量.

4. 证明实 3×3 矩阵至少有一个实特征值.

5. 求矩阵

$$\begin{bmatrix} 0 & 1 & & & \\ 1 & 0 & 1 & & \\ & 1 & \ddots & \ddots & \\ & & \ddots & & 1 \\ & & & 1 & 0 \end{bmatrix}$$

的特征多项式.

147

6. 证明命题(4.18).
7. (a) 设 T 是有两个具有同一特征值 λ 的线性无关的特征向量的线性算子. λ 是 T 的特征多项式的重根，对吗？
   (b) 设 λ 是特征多项式的重根. T 是否一定有两个具有特征值 λ 的线性无关的特征向量？
8. 设 V 是域 F 上具有基$(v_1, \cdots, v_n)$的向量空间，且设 $a_1, \cdots, a_{n-1}$ 为 F 的元素. V 上由规则$T(v_i)=v_{i+1}$ $(i<n)$和 $T(v_n)=a_1v_1+a_2v_2+\cdots+a_{n-1}v_{n-1}$定义一个线性算子.
   (a) 求 T 关于所给定的基的矩阵.
   (b) 求 T 的特征多项式.
9. A 与 A^t 有相同的特征值吗？有相同的特征向量吗？
10. (a) 用特征多项式证明所有其元素皆正的实 2×2 矩阵 P 有两个不同的实特征值.
    (b) 证明大的特征值在第一象限有一个特征向量，小的特征值在第二象限有一个特征向量.
11. (a) 设 A 是 3×3 矩阵，具有特征多项式

$$p(t) = t^3 - (\mathrm{tr}A)t^2 + s_1t - (\det A).$$

    证明 s_1 是 2×2 对称子行列式的和：

$$s_1 = \det\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \det\begin{bmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{bmatrix} + \det\begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix}.$$

   *(b) 推广到 $n\times n$ 矩阵.
12. 设 T 是 n 维空间上的线性算子，具有特征值 $\lambda_1, \cdots, \lambda_n$.
    (a) 证明 $\mathrm{tr}T=\lambda_1+\cdots+\lambda_n$ 且 $\det T=\lambda_1\cdots\lambda_n$.
    (b) 用特征值确定特征多项式的其他系数.

*13. 考虑在所有 $n\times n$ 矩阵的空间 $F^{n\times n}$上的 $n\times n$ 矩阵 A 的左乘定义的线性算子. 计算这个算子的迹和行列式.

*14. 设 P 是满足 $P^t=P^2$ 的实矩阵. P 可能的特征值是什么？

15. 设 A 是满足 $A^n=I$ 的矩阵. 证明 A 的特征值是 n 次单位根 $\xi_n=e^{\frac{2\pi i}{n}}$ 的幂.

第五节 正交矩阵与旋转

1. 绕轴 e_2 转过角度 θ 的三维旋转的矩阵是什么？
2. 证明标准正交的 n 个向量的集合是$\mathbb{R}^n$ 的一个基.
3. 用代数方法证明实 2×2 矩阵$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$代表旋转当且仅当它属于 SO_2.
4. (a) 证明 O_n 和 SO_n 是 $GL_n(\mathbb{R})$的子群，并求 SO_n 在 O_n 中的指标.
   (b) O_2 是否同构于 $SO_2\times\{\pm I\}$？O_3 是否同构于 $SO_3\times\{\pm I\}$？

148

5. 绕轴 v 转过角度 θ 的$\mathbb{R}^3$ 旋转的矩阵 A 的特征值是什么？
6. 设 A 是 O_3 中一个行列式为-1 的矩阵. 证明-1 是 A 的一个特征值.
7. 设 A 是一个正交的 2×2 矩阵，其行列式为-1. 证明 A 表示一个关于一条过原点的直线的反射.
8. 设 A 是 SO_3 的一个元素，其旋转角度为 θ. 证明 $\cos\theta=\frac{1}{2}(\mathrm{tr}\,A-1)$.

9. 每个 3 次实多项式有一个实根. 由此给出引理(5.23)的一个不太有技巧的证明.

*10. 找出一个求两个三维旋转的合成的旋转轴的几何方法.

11. 设 v 是单位长度的向量，设 P 是$\mathbb{R}^3$ 中与 v 正交的平面. 描述 P 上单位圆的点和第一列为 v 的矩阵 $P\in SO_3$ 之间的一一对应关系.

12. 给出行列式为－1 的正交矩阵作用的几何描述.

13. 证明如(5.15)定义的刚体运动是双射的.

*14. 设 A 是 SO_3 的元素. 证明如果向量

$$((a_{23}+a_{32})^{-1},(a_{13}+a_{31})^{-1},(a_{12}+a_{21})^{-1})^t$$

有定义，则它是特征值为 1 的特征向量.

第六节 对角化

1. (a)求矩阵

$$\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}$$

的特征向量和特征值.

(b)求矩阵 P，使得 PAP^{-1}是对角的.

(c)计算$\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}^{30}$.

2. 利用复数对角化旋转矩阵$\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}$.

3. 证明：如果 A，B 是 $n\times n$ 矩阵且如果 A 是非奇异的，则 AB 与 BA 相似.

4. 设 A 是以零为仅有的特征值的复矩阵，证明或推翻结论：A 是幂零的.

5. 在下列每一情形中，如果矩阵可对角化，求矩阵 P 使得 PAP^{-1}为对角的.

(a)$\begin{bmatrix}-2 & 2\\ -2 & 3\end{bmatrix}$ (b)$\begin{bmatrix}1 & i\\ -i & 1\end{bmatrix}$ (c)$\begin{bmatrix}1 & 2 & 3\\ 0 & 4 & 5\\ 0 & 0 & 6\end{bmatrix}$ (d)$\begin{bmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix}$

6. (6.1)的对角化是否可以用一个矩阵 $P\in SL_n$ 来做?

7. 证明线性算子 T 是幂零的当且仅当存在 V 的基使得 T 的矩阵为上三角形的，且对角元素都为零.

8. 设 T 是 2 维空间的线性算子. 假设 T 的特征多项式为$(t-a)^2$. 证明存在 V 的基使得 T 的矩阵具有下列两个形式之一：$\begin{bmatrix}a & 1\\ 0 & a\end{bmatrix}$，$\begin{bmatrix}a & 0\\ 0 & a\end{bmatrix}$.

149

9. 设 A 是幂零矩阵，证明 $\det(I+A)=1$.

10. 证明：若 A 是幂零的 $n\times n$ 矩阵，则 $A^n=0$.

11. 求使得 $A^2=I$ 的所有实 2×2 矩阵，用几何方法描述它们的左乘在$\mathbb{R}^2$ 上的作用.

12. 设 M是由两个对角块组成的矩阵：$M=\begin{bmatrix}A & 0\\ 0 & D\end{bmatrix}$. 证明 M是可对角化的当且仅当 A 和 D 都是可对角化的.

13. (a) 设 $A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$是有特征值$\lambda$ 的 2×2 矩阵. 证明$(b,\lambda-a)^t$ 是 A 的一个特征向量.

(b) 如果 A 有两个不同的特征值λ_1，λ_2，求矩阵 P 使得 PAP^{-1}是对角的.

14. 设 A 是复 $n\times n$ 矩阵. 证明存在任意靠近 A 的矩阵 B(意为对所有 i，j，$|b_{ij}-a_{ij}|$ 可以任意小)使得 B 有 n 个不同的特征值.

*15. 设 A 是有 n 个不同的特征值的复 $n\times n$ 矩阵．设 λ_1 是最大的特征值，即对所有 $i>1$，$|\lambda_1|>|\lambda_i|$．证明对大多数向量 X，序列 $X_k=\lambda_1^{-k}A^kX$ 收敛于有特征值 λ_1 的一个特征向量 Y，精确地描述对于 X，这一情形成立的条件是什么．

16. (a) 用上一问题中的方法计算 $\begin{bmatrix}3&1\\3&4\end{bmatrix}$ 的最大特征值，精确到三位小数．

(b) 计算矩阵 $\begin{bmatrix}1&2&3\\1&1&1\\1&0&1\end{bmatrix}$ 的最大特征值，精确到三位小数．

*17. 设 A 是 $m\times m$ 复矩阵而 B 是 $n\times n$ 复矩阵，考虑由 $T(M)=AMB$ 定义的所有复矩阵空间 $F^{m\times n}$ 上的线性算子 T．

(a) 指出如何由一对列向量 X，Y 构造 T 的特征向量，其中 X 是 A 的特征向量而 Y 是 B 的特征向量．

(b) 用 A 和 B 的特征值确定 T 的特征值．

*18. 设 A 是 $n\times n$ 复矩阵．

(a) 考虑由规则 $T(B)=AB-BA$ 定义的所有复 $n\times n$ 矩阵的空间 $F^{n\times n}$ 上的线性算子．证明这个算子的秩最多是 n^2-n．

(b) 用 A 的特征值 λ_1，…，λ_n 确定 T 的特征值．

第七节　微分方程组

1. 设 v 是矩阵 A 的一个特征向量，特征值为 c．证明 $e^{ct}v$ 是微分方程 $\frac{dX}{dt}=AX$ 的解．

2. 对下列矩阵 A，解方程 $\frac{dX}{dt}=AX$．

(a) $\begin{bmatrix}2&1\\1&2\end{bmatrix}$　(b) $\begin{bmatrix}-2&2\\-2&3\end{bmatrix}$　(c) $\begin{bmatrix}1&i\\-i&1\end{bmatrix}$　(d) $\begin{bmatrix}1&2&3\\0&4&5\\0&0&6\end{bmatrix}$　(e) $\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$

3. 解释为什么对角化能给出一般解．

4. (a) 证明命题(7.16)．

(b) 为什么只要写出实部和虚部就能得到一般解．

5. 证明引理(7.25)

6. 用齐次方程 $\frac{dX}{dt}=AX$ 的解来求解非齐次微分方程 $\frac{dX}{dt}=AX+B$．

7. 形如 $\frac{d^nx}{dt^n}+a_{n-1}\frac{d^{n-1}x}{dt^{n-1}}+\cdots+a_1\frac{dx}{dt}+a_0x=0$ 的微分方程可用如下技巧改写为一阶微分方程组：引入未知函数 x_0，x_1，…，x_{n-1} 使得 $x=x_0$，且对 $i=0,1,\cdots,n-2$，令 $\frac{dx_i}{dt}=x_{i+1}$．对 $i=0,1,\cdots,n-2$，令 $\frac{dx_i}{dt}=x_{i+1}$，并记 $\frac{dx_{n-1}}{dt}=-(a_{n-1}x_{n-1}+\cdots+a_1x_1+a_0x)$，原方程可改写为方程组．求表示这个方程组的矩阵．

8. (a) 将一个变量的二阶线性微分方程

$$\frac{d^2x}{dt^2}+b\frac{dx}{dt}+cx=0$$

写成两个变量 $x_0=x$，$x_1=\frac{dx}{dt}$ 的两个一阶方程组．

(b) 对 $b=-4$ 和 $c=3$ 解这个方程组．

9. 设 A 是 $n\times n$ 矩阵，且 $B(t)$ 是区间 $[\alpha,\beta]$ 上的连续函数的列向量．定义 $F(t)=\int_a^t e^{-sA}B(t)dt$．

(a) 证明 $X=F(t)$ 是微分方程 $X'=AX+B(t)$ 在区间 (α,β) 上的一个解．

(b) 确定这个方程在该区间上的所有解．

第八节 矩阵指数

1. 对下列矩阵 A 计算 e^A.

(a) $\begin{bmatrix} & 1 \\ -1 & \end{bmatrix}$ (b) $\begin{bmatrix} a & b \\ & \\ & \end{bmatrix}$

2. 设 $A=\begin{bmatrix} 1 & 1 \\ & 2 \end{bmatrix}$.

(a) 直接由展开式计算 e^A.

(b) 用对角矩阵计算 e^A.

3. 对下列矩阵 A，计算 e^A：

(a) $\begin{bmatrix} 0 & -b \\ b & 0 \end{bmatrix}$ (b) $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (c) $\begin{bmatrix} 0 & 1 & & & \\ & & 1 & & \\ & & \ddots & \ddots & \\ & & & & 1 \\ & & & & 0 \end{bmatrix}$

4. 对下列矩阵 A 计算 e^A：

(a) $\begin{bmatrix} 2\pi i & 2\pi i \\ & 2\pi i \end{bmatrix}$ (b) $\begin{bmatrix} 6\pi i & 4\pi i \\ 2\pi i & 8\pi i \end{bmatrix}$

151 5. 设 A 是 $n\times n$ 矩阵. 证明映射 $t \rightsquigarrow e^{tA}$ 是由加法群$\mathbb{R}^+$ 到 $GL_n(\mathbb{C})$的同态.

6. 求两个矩阵 A，B 使得 $e^{A+B}\neq e^A e^B$.

7. 证明公式 $e^{\text{trace}\, A}=\det(e^A)$.

8. 当 $A=\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$时，解微分方程$\frac{dX}{dt}=AX$.

9. 设 $f(t)$是一个多项式，并设 T 是线性算子. 证明 $f(T)$是线性算子.

10. 设 A 是对称矩阵，并设 $f(t)$是一个多项式. 证明 $f(A)$是对称的.

11. 证明矩阵值函数微分的乘积法则.

12. 设 $A(t)$，$B(t)$是 t 的可微的矩阵值函数. 计算下列微分.

(a) $\frac{d}{dt}(A(t)^3)$.

(b) $\frac{d}{dt}(A(t)^{-1})$，假设对所有 t，$A(t)$可逆.

(c) $\frac{d}{dt}(A(t)^{-1}B(t))$.

13. 设 X 是 $n\times n$ 矩阵 A 的特征向量，特征值为 λ.

(a) 证明如果 A 可逆，则 X 也是 A^{-1}的特征向量，特征值是 λ^{-1}.

(b) 设 $p(t)$是一个多项式，则 X 是 $p(A)$的特征向量，特征值是 $p(\lambda)$.

(c) 证明 X 是 e^A 的特征向量，特征值是 e^λ.

14. 对 $n\times n$ 矩阵 A，用 $\sin x$ 和 $\cos x$ 的泰勒级数展开式定义 $\sin A$ 和 $\cos A$.

(a) 证明对所有 A，这些级数收敛.

(b) 证明 $\sin tA$ 是 t 的可微函数，且$\frac{d(\sin tA)}{dt}=A\cos tA$.

15. 讨论下列恒等式成立的范围.

(a) $\cos^2 A+\sin^2 A=I$.

(b) $e^{iA}=\cos A+i\sin A$.

(c) $\sin(A+B)=\sin A\cos B+\cos A\sin B$.

(d) $\cos(A+B)=\cos A\cos B-\sin A\sin B$.

(e) $e^{2\pi iA}=I$.

(f) $\frac{d(e^{A(t)})}{dt}=e^{A(t)}A'(t)$，其中 $A(t)$是 t 的可微的矩阵值函数.

16. (a) 用两种方法导出复值函数微分的乘积法则：直接计算以及将其写作 $x(t)=u(t)+iv(t)$并应用实值函数的乘积法则.

(b) 设 $f(t)$是实变量 t 的复值函数，并设 $\varphi(u)$是 u 的实值函数. 叙述并证明 $f(\varphi(u))$的链式法则.

17. (a) 设 B_k 是收敛于矩阵 B 的一个 $m\times n$ 矩阵序列，并设 P 是一个 $m\times m$ 矩阵. 证明 PB_k 收敛于 PB.

(b) 证明如果 $m=n$ 且 P 可逆，则 PB_kP^{-1}收敛于 PBP^{-1}.

18. 设 $f(x)=\sum c_kx^k$ 是一个幂级数，对充分小的 $n\times n$ 矩阵 A，$\sum c_kA^k$ 收敛. 证明 A 与$f(A)$交换.

19. 当 $A(t)$是 t 的一个可微矩阵函数，确定$\frac{d}{dt}\det A(t)$.

杂题

1. 什么是满足下列条件的线性算子 T 的可能的特征值？

(a) $T^r=I$ (b) $T^r=0$ (c) $T^2-5T+6=0$

[152]

2. 线性算子 T 称为幂零的，如果 T 的某个幂为零.

(a) 证明 T 是幂零的当且仅当其特征多项式是 t^n，$n=\dim V$.

(b) 证明如果 T 是 n 维向量空间的幂零算子，则 $T^n=0$.

(c) 线性算子 T 称为幂单的，如果 $T-I$ 是幂零的. 求幂单算子的特征多项式，可能的特征值是什么？

3. 设 A 是一个 $n\times n$ 复矩阵. 证明如果对所有 i 有迹 $\operatorname{trace}A^i=0$，则 A 是幂零的.

*4. 设 A，B 是复 $n\times n$ 矩阵，并设 $C=AB-BA$. 证明如果 C 与 A 交换，则 C 是幂零的.

5. 设 λ_1，…，λ_n 是复矩阵 A 的特征多项式 $p(t)$的根. 证明公式 $\operatorname{trace}A=\lambda_1+\cdots+\lambda_n$ 和 $\det A=\lambda_1\cdots\lambda_n$.

6. 设 T 是实向量空间 V 上的线性算子，满足条件 $T^2=I$. 定义子空间如下：

$$W^+=\{v\in V\mid T(v)=v\},\quad W^-=\{v\in V\mid T(v)=-v\}.$$

证明 V 同构于直和 $W^+\oplus W^-$.

7. $n\times n$ 矩阵 A 的弗罗贝尼乌斯范数 $|A|$ 定义为将 A 视为 n^2-维向量时 A 的长度：$|A|^2=\sum|a_{ij}|^2$. 证明不等式 $|A+B|\leqslant|A|+|B|$ 及 $|AB|\leqslant|A||B|$.

8. 设 $T: V\longrightarrow V$ 是有限维向量空间 V 的一个线性算子. 证明存在整数 n，使得$(\ker T^n)\cap(\operatorname{im}T^n)=0$.

9. 哪些无限矩阵代表空间 Z[第三章(5.2d)]的线性算子？

*10. $m\times n$ 矩阵 A 的 $k\times k$ 子式是由划去 $m-k$ 行和 $n-k$ 列后得到的子矩阵. 设 A 是秩 r 的矩阵. 证明某个 $r\times r$ 子式可逆，并且没有可逆的$(r+1)\times(r+1)$子式.

11. 设 $\varphi: F^n\longrightarrow F^m$ 是用 $m\times n$ 矩阵 A 左乘. 证明下列叙述等价.

(a) A 有右逆，即存在一个矩阵 B 使得 $AB=I$.

(b) φ 是满射.

(c) A 有一个 $m\times m$ 子式，其行列式不为零.

12. 设 $\varphi: F^n\longrightarrow F^m$ 是用 $m\times n$ 矩阵 A 左乘. 证明下列叙述等价.

(a) A 有左逆，即存在一个矩阵 B 使 $BA=I$.

(b) φ 是单射.

(c) A有一个$n\times n$子式，其行列式非零.

*13. 设A是一个$n\times n$矩阵且$A^r=I$. 证明如果A只有一个特征值ξ，则$A=\xi I$.

14. (a) 不用特征多项式，证明n维向量空间的一个线性算子最多有n个不同的特征值.

(b) 用(a)证明系数在域F中的n次多项式在F中最多有n个根.

15. 设A是一个$n\times n$矩阵，且设$p(t)=t^n+c_{n-1}t^{n-1}+\cdots+c_1t+c_0$是它的特征多项式. 凯莱-哈密顿定理断言

$$p(A)=A^n+c_{n-1}A^{n-1}+\cdots+c_1A+c_0I=0.$$

(a) 对2×2矩阵证明凯莱-哈密顿定理.

153 (b) 对对角矩阵证明这个定理.

(c) 对可对角化的矩阵证明这个定理.

*(d) 证明每个复$n\times n$矩阵任意靠近一个可对角化矩阵，并用这一事实将可对角化矩阵的证明用连续性拓广到任意复矩阵.

16. (a) 利用凯莱-哈密顿定理给出一个A^{-1}由A，$(\det A)^{-1}$和特征多项式的系数的表示的表达式.

(b) 在2×2的情形通过直接计算验证这个表达式.

*17. 设A是2×2矩阵. 凯莱-哈密顿定理指出能将A的所有的幂写成I和A的线性组合. 因而e^A亦是一个这样的线性组合.

(a) 证明：如果a，b是A的特征值且如果$a\neq b$，则

$$e^A=\frac{a e^b-b e^a}{a-b}I+\frac{e^a-e^b}{a-b}A.$$

(b) 在A有两个相等的特征值时，找到正确的公式.

18. 斐波那契数0，1，1，2，3，5，8，…是在初始条件$f_0=0$，$f_1=1$之下由迭代关系$f_n=f_{n-1}+f_{n-2}$定义. 迭代关系可用矩阵形式写为

$$\begin{bmatrix}0&1\\1&1\end{bmatrix}\begin{bmatrix}f_{n-2}\\f_{n-1}\end{bmatrix}=\begin{bmatrix}f_{n-1}\\f_n\end{bmatrix}.$$

(a) 证明公式

$$f_n=\frac{1}{\alpha}\left[\left(\frac{1+\alpha}{2}\right)^n-\left(\frac{1-\alpha}{2}\right)^n\right],$$

其中$\alpha=\sqrt{5}$.

(b) 设序列a_n由关系$a_n=\frac{1}{2}(a_{n-1}+a_{n-2})$定义，用$a_0$，$a_1$计算$\lim a_n$.

*19. 设A是一个正的实$n\times n$矩阵，$X\in\mathbb{R}^n$是一个列向量. 我们用简写记号$X>0$或$X\geqslant 0$分别表示向量X的分量是正的或非负的. "正象限"是指向量$X\geqslant 0$的集合.（$X\geqslant 0$但$X\neq 0$在我们的意义下不能得到$X>0$）.

(a) 证明若$X\geqslant 0$且$X\neq 0$，则$AX>0$.

(b) 设C表示满足条件$X\geqslant 0$，$|X|=1$且$(A-tI)X\geqslant 0$的对$(X,t)(t\in\mathbb{R})$的集合. 证明C在$\mathbb{R}^{n+1}$中是紧的.

(c) 函数t在C中，比如说在点(X_0,t_0)取极大值. 则$(A-t_0I)X_0\geqslant 0$. 证明$(A-t_0I)X_0=0$.

(d) 证明X_0是特征值为t_0的特征向量，否则向量$AX_0=X_1$将与t_0的极大性相矛盾.

(e) 证t_0是A的绝对值最大的特征值.

*20. 设$A=A(t)$是函数矩阵，当类似$n=1$时，试图证明矩阵

$$\exp\left(\int_{t_0}^{t}A(u)\,du\right)$$

154 是方程组$\frac{dX}{dt}=AX$的解时什么地方出了错？你能对矩阵函数$A(t)$找到使这成为一个解的条件吗？

第五章　对　　称

代数不是写出的几何，几何也不是画出的代数.

Sophie Germain

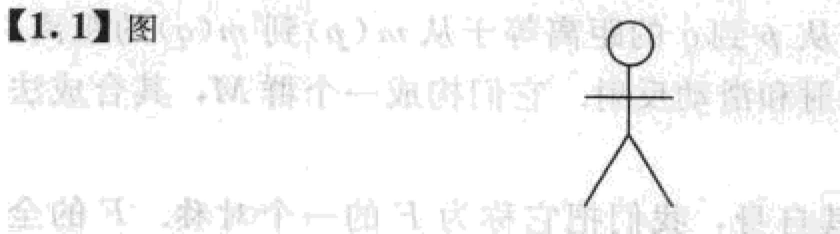
对称为群论提供了最引人入胜的应用. 群最早是为了分析称为扩域的代数结构的对称性而发明的，因为对称性是所有科学中一个共同的现象，所以它仍是群论应用的两个主要方式之一. 另一个应用方式是通过群的表示，我们将在第九章加以讨论. 本章前四节，我们将用平面刚体运动群的语言研究平面图形的对称. 平面图形为第五节引入的群作用的一般概念提供了丰富的实例和背景.

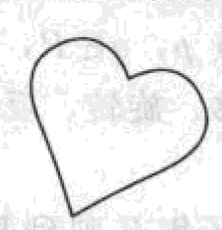
当研究对称时，我们将允许使用几何推理而不必回溯到几何公理. 那将留到其他场合.

第一节　平面图形的对称

平面图形可能的对称通常可分为图(1.1)～(1.3)所示的几种主要类型.

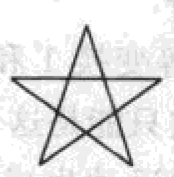
【1.1】 图

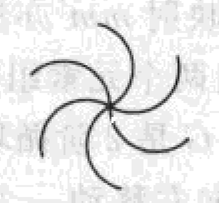




双侧对称

【1.2】 图





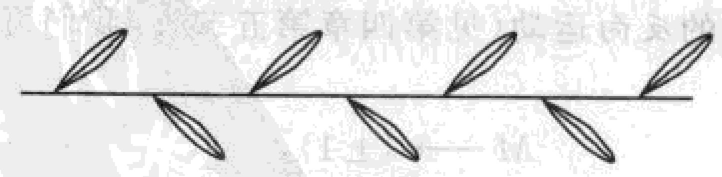
旋转对称

【1.3】 图

平移对称

还存在我们不太熟悉的第四类对称.

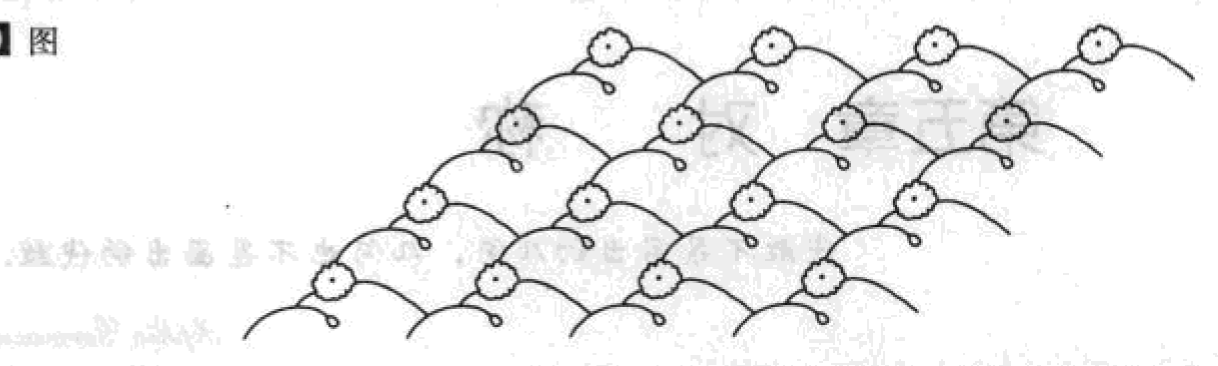
【1.4】 图



滑动对称

像墙纸图案这样的图形可以有两个独立的平移对称，如图(1.5)所示.

【1.5】图



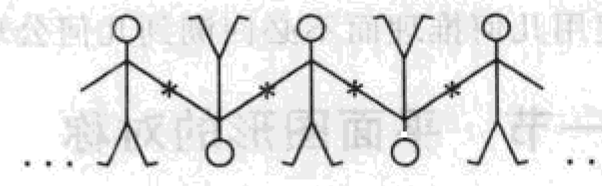
其他对称的组合也可能发生. 例如，星形图案具有双侧对称和旋转对称. 图(1.6)是平移对称和旋转对称组合起来的例子：

【1.6】图

honeyhoneyhoney…

另一个例子如图(1.7)所示.

【1.7】图



156

如第四章第五节所示，平面 P 到自身的映射 m：$P \longrightarrow P$ 称为一个刚体运动或一个等距，如果它是保持距离的，即对任意两点 p，$q \in P$，从 p 到 q 的距离等于从 $m(p)$ 到 $m(q)$ 的距离. 在下一节我们将证明刚体运动是平移、旋转、反射和滑动反射. 它们构成一个群 M，其合成法则为函数合成.

如果刚体运动 m 将平面的一个子集 F 映到其自身，我们把它称为 F 的一个对称. F 的全体对称的集合 G 总是构成 M 的子群 G，称为该图形的*对称群*. G 是子群的这一事实是显然的：如果 m 和 m' 将 F 映到 F，则合成映射 mm' 亦然，等等.

双侧对称图形(1.1)的对称群由两个元素组成：恒等变换 1 和关于一条称为对称轴的直线的反射 r. 我们有关系 $rr=1$，这表明 G 是 2 阶循环群，它只能是这个群，因为没有别的 2 阶群.

图形(1.3)的对称群是由使其向左移动一个单位的运动生成的一个无限循环群. 我们称这样一个运动为一个*平移* t：

$$G = \{\cdots, t^{-2}, t^{-1}, 1, t^{1}, t^{2}, \cdots\}.$$

图(1.4)、(1.6)、(1.7)的对称群除了平移外还含有其他元素，因而更大. 作为练习请描述其元素.

第二节 平面运动群

本节描述平面的全体刚体运动的群 M. 运动的最粗糙的分类是将其分为不使平面翻转过来的保向运动和使平面翻转过来的反向运动(见第四章第五节). 我们可以用 M 的这个划分定义一个映射

$$M \longrightarrow \{\pm 1\},$$

将保向运动映到 1 而将反向运动映到 -1. 读者不难看出这个映射是一个同态：两个反向运动

的乘积是保向的，等等.

运动的一个更为精细的分类如下：

【2.1】

(a) 保向运动：

(i) 平移：由一个向量 a：$p \rightsquigarrow p+a$ 给出的平面的平行运动.

(ii) 旋转：平面绕某个点转过一个角度 $\theta(\theta \neq 0)$.

(b) 反向运动：

(i) 关于直线 ℓ 的反射.

(ii) 滑动反射：先关于直线 ℓ 反射，然后平移一个与 ℓ 平行的非零向量 a.

157

【2.2】定理 上面所列出的分类是完全的. 每个刚体运动或为一个平移，或为一个旋转，或为一个反射，或为一个滑动反射，或为一个恒等映射.

这个定理是非常重要的. 它的一个直接推论是，围绕两个不同点的旋转的合成如果不是平移，便一定是围绕第三个点的一个旋转. 因为这样的合成是保向的，由定理就可以得到这个事实，但它并不是明显的.

某些其他合成是容易看出的. 绕同一个点转过角度 θ 和 η 的旋转的合成是绕同一点转过角度 $\theta+\eta$ 的旋转. 由向量 a，b 得到的平移的合成是由 $a+b$ 得到的平移.

注意平移不能使任何一个点不动(除非向量 a 为零，这时是恒等映射). 滑动也没有不动点. 另一方面，旋转恰有一个点不动，即旋转的中心，反射保持反射直线上的点不动. 因而关于两条不平行的直线 ℓ_1，ℓ_2 的反射的合成是一个围绕其交点 $p=\ell_1 \cap \ell_2$ 的旋转. 这可由定理得到，因为合成的确使 p 不变，且是保向的. 关于平行直线的两个反射的合成是由一个与直线垂直的向量决定的平移.

为了证明定理(2.2)，也是为了能在群 M 中方便地计算，我们将选择一些特殊的运动作为群的生成元. 我们将得到类似于第二章中定义对称群 S_3 的关系(1.18)的定义关系，但由于 M 是无限的，因此将需要更多的生成元和关系.

通过选择坐标系，我们将平面等同于列向量空间$\mathbb{R}^2$. 这时，我们选择平移、围绕原点的旋转和关于 x_1 轴的反射作为生成元：

【2.3】

(a) 由向量 a 给出的平移 t_a：$t_a(x)=x+a=\begin{bmatrix} x_1+a_1 \\ x_2+a_2 \end{bmatrix}$.

(b) 围绕原点转过角度 θ 的旋转 ρ_θ：

$$\rho_\theta(x)=\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

(c) 关于 x_1 轴的反射 r：$r(x)=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}=\begin{bmatrix} x_1 \\ -x_2 \end{bmatrix}$.

由于旋转 ρ_θ 和反射 r 保持原点不动，因此它们都是$\mathbb{R}^2$ 的正交算子. 平移不是线性算子——除了零向量给出的平移，它不将零向量映到自身.

(2.3) 列出的运动并不是 M 的全部元素. 例如, 围绕原点之外的点的旋转就不在其列, 关于其他直线的反射也没有. 然而, 它们的确生成了这样的群: M 中每个元素是这样元素的乘积. 容易看出, 任意刚体运动 m 可以由它们的合成得到.

158

【2.4】
$$m = t_a\rho_\theta \quad 或 \quad m = t_a\rho_\theta r,$$
对某个可能为零的向量 a 和角度 θ 成立. 为此, 我们先回忆每个刚体运动都是正交算子跟上一个平移的合成[第四章(5.20)]. 因而, 我们可以将 m 写为 $m=t_am'$, 其中 m' 是一个正交算子. 其次, 若 $\det m'=1$, 则它是一个旋转 ρ_θ. 这由第四章定理(5.5)推出. 因而在这种情形, $m=t_a\rho_\theta$. 最后, 若 $\det m'=-1$, 则 $\det m'r=1$, 因此 $m'r$ 是一个旋转 ρ_θ. 因为 $r^2=1$, 这时 $m'=\rho_\theta r$, 因而 $m=t_a\rho_\theta r$.

运动 m 作为乘积(2.4)的表达式是唯一的. 若 m 可由两种方式表达: $m=t_a\rho_\theta r^i=t_b\rho_\eta r^j$, 其中 i, j 为 0 或 1. 因为当 $i=0$ 时 m 保向而当 $i=1$ 时 m 反向, 我们必有 $i=j$, 因而在必要时可在两边消去 r 得到等式 $t_a\rho_\theta=t_b\rho_\eta$. 两边左乘 t_{-b} 右乘 $\rho_{-\theta}$ 得 $t_{a-b}=\rho_{\eta-\theta}$. 但除了二者都是平凡作用时, 平移不能等于旋转. 因而 $a=b$ 且 $\theta=\eta$.

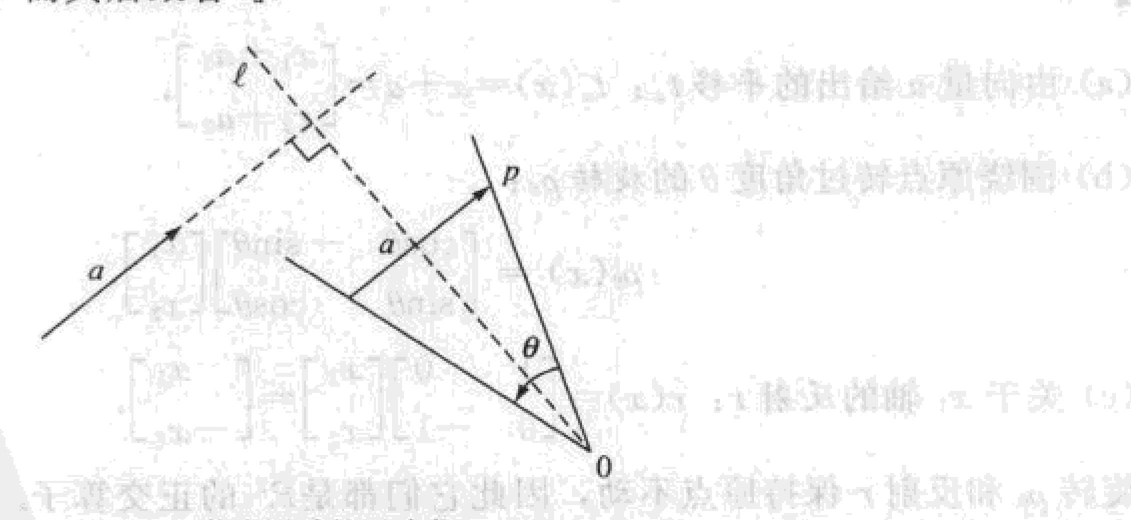
M 中的计算可以用符号 t_a, ρ_θ, r 进行, 用公式(2.3)算出合成它们的规则. 这些必要的规则是:

【2.5】
$$t_at_b = t_{a+b}, \quad \rho_\theta\rho_\eta = \rho_{\theta+\eta}, \quad rr = 1,$$
$$\rho_\theta t_a = t_{a'}\rho_\theta, \quad 其中\ a' = \rho_\theta(a),$$
$$rt_a = t_{a'}r, \quad 其中\ a' = r(a),$$
$$r\rho_\theta = \rho_{-\theta}r.$$
利用这些规则, 可将生成元的任意乘积化为(2.4)中两种形式之一. 得到的形式是唯一确定的, 因为每个给定的运动只有一个形如(2.4)的表达式.

定理(2.2)的证明 设 m 是一个保向但不是平移的刚体运动. 我们要证明 m 是围绕某个点的旋转. 很显然, 保持平面上点 p 不动的保向运动必为围绕点 p 的旋转. 因此要证明每个非平移的保向运动必保持某个点不动. 如(2.4)我们记 $m=t_a\rho_\theta$. 由假设, $\theta\neq 0$. 我们可用图(2.6)中的几何图形找到不动点. 其中 ℓ 是过原点且与 a 垂直的直线. 取适当位置使夹角为 θ 的扇形能被 ℓ 平分. p 可以如图所示通过将向量 a 插入扇形得到. 要证明 m 保持 p 不动, 只需记住作用 ρ_θ 是我们的第一个运动, 而其后跟着 t_a.

159

【2.6】 图



保向运动的不动点

求不动点的另一个方法是用代数方法关于 x 求解方程 $x=t_a\rho_\theta(x)$. 按平移的定义，$t_a(\rho_\theta(x))=\rho_\theta(x)+a$. 因而我们要解的方程是

$$x-\rho_\theta(x)=a \quad \text{或}$$

【2.7】
$$\begin{bmatrix}1-\cos\theta & \sin\theta \\ -\sin\theta & 1-\cos\theta\end{bmatrix}\begin{bmatrix}x_1 \\ x_2\end{bmatrix}=\begin{bmatrix}a_1 \\ a_2\end{bmatrix}.$$

注意 $\det(1-\rho_\theta)=2-2\cos\theta$. 当 $\theta\neq 0$ 时行列式非零，因而关于 x 有唯一解.

【2.8】推论　*运动 $m=t_a\rho_\theta$ 是围绕其不动点转过角度 θ 的旋转.*

证明　如我们刚看到的，m 的不动点是满足关系 $p=\rho_\theta(p)+a$ 的那个点. 于是对任意 x，

$$m(p+x)=t_a\rho_\theta(p+x)=\rho_\theta(p+x)+a$$
$$=\rho_\theta(p)+\rho_\theta(x)+a=p+\rho_\theta(x).$$

这样 m 将 $p+x$ 映到 $p+\rho_\theta(x)$. 因而它是围绕 p 转过角度 θ 的旋转，这正是所需证明的.

其次，要证明任意反向运动 $m=t_a\rho_\theta r$ 是一个滑动反射或一个反射(我们将它看作滑动向量为零的滑动反射). 我们这样做，找一条由 m 映到自身的直线 ℓ，因而 m 在 ℓ 上的运动是平移. 几何上很清楚，在一条直线上以这种方式进行的反向运动是滑动反射.

这里几何更为复杂，我们将分两步简化问题. 首先，运动 $\rho_\theta r=r'$ 是关于一条直线的反射. 该直线是在原点处与 x_1 轴相交夹角为 $\frac{1}{2}\theta$ 的那条直线. 从代数上或从几何上这都容易看出. 这样运动 m 是平移 t_a 与反射 r' 的乘积. 我们可转动坐标系，使得 x_1 轴是反射 r' 的直线. 则 r' 成为标准反射 r，而平移 t_a 仍为平移，虽然向量 a 的坐标将会改变. 在新坐标系下，运动写为 $m=t_ar$，其作用为　[160]

$$m\begin{bmatrix}x_1 \\ x_2\end{bmatrix}=\begin{bmatrix}x_1+a_1 \\ -x_2+a_2\end{bmatrix}.$$

这个运动通过平移 $\left(x_1, \frac{1}{2}a_2\right)^t \rightsquigarrow \left(x_1+a_1, \frac{1}{2}a_2\right)^t$ 将直线 $x_2=\frac{1}{2}a_2$ 映为自身，因而 m 是沿此直线的滑动. ■

M 有两个重要的子群，我们为它们引入记号：

【2.9】T，平移群.

　　$\boldsymbol{O}$，正交算子群.

群 $\boldsymbol{O}$ 由使原点保持不动的运动组成. 它包含围绕原点的旋转和关于过原点的直线的反射.

注意根据坐标系的选择，我们得到一个一一对应

【2.10】
$$\mathbb{R}^2 \longrightarrow T$$
$$a \rightsquigarrow t_a.$$

因为 $t_at_b=t_{a+b}$，所以这是加法群 $(\mathbb{R}^2)^+$ 与子群 T 的一个同构.

$\boldsymbol{O}$ 的元素是线性算子. 再次用我们坐标的选择，可将一个元 $m\in\boldsymbol{O}$ 与它的矩阵相联系. 这

样，我们得到一个由正交 2×2 矩阵的群 O_2 到 $\boldsymbol{O}$ 的同构[见第四章(5.16)]

$$O_2 \xrightarrow{\sim} \boldsymbol{O}.$$

我们亦可考虑 M 中使平面上一个非原点的点为不动点的运动的子群. 这个子群与 $\boldsymbol{O}$ 的关系如下：

【2.11】命题

(a) 设 p 是平面上一点. 设 ρ'_θ 表示围绕 p 转过角度 θ 的旋转，r' 表示关于过 p 点与 x 轴平行的直线的反射. 则 $\rho'_\theta = t_p\rho_\theta t_p^{-1}$ 且 $r' = t_p r\, t_p^{-1}$.

(b) 保持 p 不动的运动的 M 中的子群是共轭子群

161

$$\boldsymbol{O}' = t_p \boldsymbol{O}\, t_p^{-1}.$$

证明 我们可以这样得到旋转 ρ'_θ：先将 p 平移到原点，然后将平面做围绕原点转过角度 θ 的旋转，最后将原点平移回到 p：

$$\rho'_\theta = t_p\rho_\theta t_{-p} = t_p\rho_\theta t_p^{-1}.$$

反射 r' 可由 r 用同样的方式得到：

$$r' = t_p\, r\, t_{-p} = t_p\, r\, t_p^{-1}.$$

这证明了(a). 因为每个保持 p 不动的运动具有 ρ'_θ 或 $\rho'_\theta r'$ 的形式[见(2.4)的证明]，所以(b)由(a)得到. ■

存在一个从 M 到 $\boldsymbol{O}$，并且其核为 T 的重要的同态 φ，它由在积(2.4)中去掉平移得到：

$$M \xrightarrow{\varphi} \boldsymbol{O}$$

【2.12】

$$t_a\rho_\theta \rightsquigarrow \rho_\theta$$

$$t_a\rho_\theta r \rightsquigarrow \rho_\theta r.$$

这看起来可能太过直观而不是一个好定义，但公式(2.5)指出 φ 是一个同态：$(t_a\rho_\theta)(t_b\rho_\eta) = t_a t_{b'}\rho_\theta\rho_\eta = t_{a+b'}\rho_{\theta+\eta}$，因而 $\varphi(t_a\rho_\theta t_b\rho_\eta) = \rho_{\theta+\eta}$，等等. 因为 T 是同态的核，所以它是 M 的正规子群.

注意，我们不能用这样的方式定义 M 到 T 的同态.

【2.13】命题 设 p 是平面上的任意点，并设 ρ'_θ 表示围绕 p 转过角度 θ 的旋转. 则 $\varphi(\rho'_\theta) = \rho_\theta$. 类似地，若 r' 是关于过 p 点与 x 轴平行的直线的反射，则 $\varphi(r') = r$.

这由(2.11a)得到，因为 t_p 属于 φ 的核. 命题亦可如下表述：

【2.14】同态 φ 与原点选择无关.

第三节 有限运动群

本节研究如(1.1)和(1.2)的对称图形组成的可能的有限群. 这样我们将被引向对平面刚体运动群 M 的有限子群 G 的研究.

描述所有的有限子群的关键是下面的定理.

【3.1】定理　*不动点定理：设 G 是运动群 M 的有限子群．存在平面上的一个点 p，它在 G 的每个元素作用之下不动，即存在点 p 使得对所有 $g\in G$ 有 $g(p)=p$.*

162

由此可得，例如，M 的任一含有绕两个不同点的旋转的任意子群皆是无限的.

下面是定理的一个漂亮的几何证明．设 s 是平面上的任意点，并设 S 是在 G 中各个运动作用下 s 的象点的集合．因而每个元素 $s'\in S$ 对某个 $g\in G$ 有 $s'=g(s)$．这个集合称为 s 在 G 作用下的轨道．元素 s 属于轨道，因为单位元 1 在 G 中，且 $s=1(s)$．一个典型的轨道如下图所示，此时 G 是正五边形对称群.

保向运动的不动点

群 G 的任意元素都将置换轨道 S．换言之，若 $s'\in S$ 且 $x\in G$，则 $x(s')\in S$．比如 $s'=g(s)$，$g\in G$. 因为 G 是群，$xg\in G$．于是由定义，$xg(s)\in S$．因为 $xg(s)=x(s')$，这就证明了 $x(s')\in S$.

我们任意排列 S 的元素，记 $S=\{s_1,\cdots,s_n\}$．所求的不动点是轨道的重心，定义为

【3.2】
$$p=\frac{1}{n}(s_1+\cdots+s_n),$$

其中右边可以在平面上的任一坐标系下用向量加法计算．重心应视为点 $s_1,\cdots,s_n$ 的一个平均.

【3.3】引理　*设 $S=\{s_1,\cdots,s_n\}$ 是平面上一个有限点集，并设 p 为其重心，由(3.2)定义．设 m 是一个刚体运动，并设 $m(s_i)=s'_i$ 和 $m(p)=p'$．则 $p'=\frac{1}{n}(s'_1+\cdots+s'_n)$．换言之，刚体运动将重心变到重心.*

证明　物理上的论证是清楚的，也可通过计算证明．为此，只要分别处理 $m=t_a$，$m=\rho_\theta$ 以及 $m=r$ 的情形，这是因为任何一个运动可以由其合成得到.

情形 1：$m=t_a$，则 $p'=p+a$ 且 $s'_i=s_i+a$．事实上有

$$p+a=\frac{1}{n}((s_1+a)+\cdots+(s_n+a)).$$

情形 2：$m=\rho_\theta$ 或 r．这时 m 是线性算子，因而

163

$$p'=m\left(\frac{1}{n}(s_1+\cdots+s_n)\right)=\frac{1}{n}(m(s_1)+\cdots+m(s_n))=\frac{1}{n}(s'_1+\cdots+s'_n).$$

集合 S 的重心是 G 的作用的不动点．因为 G 的任意元 g_i 置换轨道 $\{s_1,\cdots,s_n\}$，于是引理(3.3)指出它将重心变为自己．这就完成了定理的证明. ■

现设 G 是 M 的一个有限子群．定理(3.1)告诉我们存在一个点，它是 G 的每个元素的不动点，可以调整坐标系使这个点为原点．于是 G 将成为 $\boldsymbol{O}$ 的子群．因此要描述 M 的有限子群 G，

只需描述 $\boldsymbol{O}$ 的有限子群(或者，由于 $\boldsymbol{O}$ 同构于正交 2×2 矩阵群，只需描述正交群 O_2 的有限子群). 这些子群由下面的定理描述.

【3.4】定理 设 G 是保持原点不变的刚体运动的群 $\boldsymbol{O}$ 的一个有限子群. 则 G 是下面的群之一：

(a) $G=C_n$：n 阶循环群，由旋转 ρ_θ 生成，其中 $\theta=\dfrac{2\pi}{n}$.

(b) $G=D_n$：$2n$ 阶二面体群，由两个元素生成——一个由旋转 ρ_θ 生成，其中 $\theta=\dfrac{2\pi}{n}$，另一个由关于过原点的直线的反射 r' 生成.

这个定理的证明在本节结尾处.

群 D_n 与反射的直线有关，当然，可选择坐标系而使之成为 x 轴，于是 r' 成为标准反射. 若 G 是 M 中的有限子群，则也需要将原点移动到其不动点，以便应用定理(3.4). 我们关于有限运动群的最终结果是下面的推论：

【3.5】推论 设 G 是运动群 M 的一个有限子群. 若适当地引入坐标系，则 G 成为群 C_n 或 D_n 之一，其中 C_n 由 $\rho_\theta\left(\theta=\dfrac{2\pi}{n}\right)$ 生成，而 D_n 由 ρ_θ 和 r 生成.

当 $n\geqslant3$，二面体群 D_n 是正 n 边形的对称群. 这是容易看出的，事实上，它可以由定理得到. 因为正 n 边形具有一个包含围绕其中心转过 $\dfrac{2\pi}{n}$ 角度的旋转的对称群. 同时，它也包含某个反射. 因而定理(3.4)告诉我们它是 D_n.

二面体群 D_1，D_2 太小了，不能成为一个通常意义下的 n 边形的对称群. D_1 是两个元素的群 $\{1, r\}$. 因而它是循环群，如 C_2. 但 D_1 的非平凡元素是反射，而 C_2 的是转过角度 π 的旋转. 群 D_2 含有四个元素 $\{1, \rho, r, \rho r\}$，其中 $\rho=\rho_\pi$. 它同构于克莱因四元素群. 我们可以把 D_1 和 D_2 想象成正一边形和正二边形的对称群.

164

二面体群是重要的例子，得到其定义关系的完全集合是很有用的. 它们可以从 M 的定义关系表(2.5)中读出. 我们用 x 表示旋转 $\rho_\theta\left(\theta=\dfrac{2\pi}{n}\right)$，用 y 表示反射 r.

【3.6】命题 二面体群 D_n 由两个元素 x，y 生成，满足关系

$$x^n=1,\quad y^2=1,\quad yx=x^{-1}y.$$

D_n 的元素为

$$\{1,x,x^2,\cdots,x^{n-1};y;xy,x^2y,\cdots,x^{n-1}y\}=\{x^iy^j\mid 0\leqslant i<n,\quad 0\leqslant j<2\}.$$

证明 由二面体群的定义，元素 $x=\rho_\theta$ 和 $y=r$ 生成 D_n. 关系 $y^2=1$ 和 $yx=x^{-1}y$ 包含在 M 的关系表(2.5)中：它们是 $rr=1$ 和 $r\rho_\theta=\rho_{-\theta}r$. 关系 $x^n=1$ 由事实 $\theta=\dfrac{2\pi}{n}$ 得到，这也告诉我们元素 1，x，x^2，…，x^{n-1} 互不相同. 从而也得到元素 y，xy，x^2y，…，$x^{n-1}y$ 互不相同，

且因为它们是反射而 x 的幂为旋转，所以列出的元素没有重复. 最后，可用关系将 x，y，x^{-1}，y^{-1}的任意乘积化为 x^iy^j 的形式，其中 $0\leqslant i<n$，$0\leqslant j<2$. 因此，列表中含有由 x，y 生成的子群的所有元素，而且因为这些元素生成 D_n，所以列表是完全的. ■

164

使用(3.6)的前面两个关系，第三个关系可以用不同的方式写出. 它等价于

【3.7】 $$yx = x^{n-1}y,\quad \text{也等价于}\quad xyxy = 1.$$

注意当 $n=3$ 时，这些关系与对称群 S_3 的关系[第二章(1.18)]是一样的.

【3.8】推论 *二面体群 D_3 与对称群 S_3 同构.*

对于 $n>3$，二面体群与对称群一定是不同构的，因为 D_n 的阶是 $2n$ 而 S_n 的阶是 $n!$.

定理(3.4)的证明 设 G 是 $\boldsymbol{O}$ 的有限子群. 我们要记住 $\boldsymbol{O}$ 的元素是旋转 ρ_θ 和反射 $\rho_\theta r$.

情形 1：G 的所有元素都是旋转. 我们要证明在这种情形中 G 是循环群. 证明类似于确定整数加法群$\mathbb{Z}^+$的子群[第二章(2.3)]. 若 $G=\{1\}$，则 $G=C_1$. 否则，G 有一个非平凡旋转 ρ_θ. 令 θ 为 G 的元素中旋转转过的最小正角度. 则 G 由 ρ_θ 生成. 设 ρ_α 为 G 的任一元素，其中旋转的角度 α 由一个实数代表. 设 $n\theta$ 是比 α 小的最大的 θ 的整数倍，则 $\alpha=n\theta+\beta$，且 $0\leqslant\beta<\theta$. 因为 G 是群，且 ρ_α 和 ρ_θ 属于 G，于是积 $\rho_\beta=\rho_\alpha\rho_{-n\theta}$ 亦属于 G. 但由假设，θ 是 G 中旋转的最小正角度. 于是 $\beta=0$ 而 $\alpha=n\theta$. 这就证明了 G 是循环群. 设 $n\theta$ 是 θ 的 $\geqslant 2\pi$ 的最小倍数，于是 $2\pi\leqslant n\theta<2\pi+\theta$. 因为 θ 是 G 中旋转的最小正角度，$n\theta=2\pi$. 这样 $\theta=\frac{2\pi}{n}$对某个整数 n 成立.

165

情形 2：G 含有反射. 必要时调整坐标系，我们可假定标准反射 r 属于 G. 设 H 表示 G 中由旋转构成的子群. 可将情形 1 中证明的结论应用于群 H，得到它是一个循环群：$H=C_n$. 于是 $2n$ 个积 ρ_θ^i，$\rho_\theta^i r$ $(0\leqslant i\leqslant n-1)$ 都属于 G，因而 G 包含二面体群 D_n. 我们需要证明 $G=D_n$. 现在如果 G 的一个元素 g 是旋转，则由 H 的定义有 $g\in H$；因而 g 是 D_n 的元素之一. 若 g 是一个反射，可记之为 $\rho_\alpha r$，其中 ρ_α 是旋转(3.8). 因为 $r\in G$，从而积 $\rho_\alpha rr=\rho_\alpha$. 因而 ρ_α 为 ρ_θ 的幂，且 g 亦属于 D_n. 于是 $G=D_n$. 这就完成了定理的证明. ■

第四节 离散运动群

本节讨论诸如墙纸图案等无界图形的对称群. 我们的第一个任务是描述一个条件，用来替代群是有限的这一条件——使之能够包括有趣的无界图形的对称群. 文中图案的一个性质是它们不允许任意小的平移和旋转. 对于非常特殊的图形，例如直线有任意小的平移对称，而圆有任意小的旋转对称. 如果把这些图形排除在外，就可以把对称群进行分类.

【4.1】定义 *运动群 M 的一个子群 G 称为是离散的，如果它不包含任意小的平移和旋转. 更准确地，G 是离散的，如果存在某个实数 $\varepsilon>0$ 使得*

(i) 如果 t_a 是 G 中由非零向量 a 产生的平移，则 a 的长度至少为 ε：$|a|\geqslant\varepsilon$.

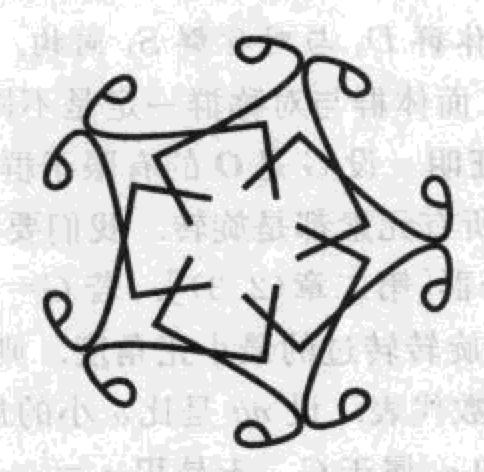
(ii) 如果 ρ 是 G 中围绕某点转过非零角度 θ 的旋转，则角度至少为 ε：$|\theta|\geqslant\varepsilon$.

因为平移和旋转都是保向运动(2.1)，这些条件亦应用于 G 的所有保向元素. 我们没对反射和滑动附加条件. 由对保向运动所加的条件自动得到它们的条件.

万花筒原理可用来证明每一个离散运动群是平面图形的对称群. 我们不准备给出精确的

推导来证明这一点，但讨论的方法可以演变成一个证明．从平面上一个充分随机的图形 R 开始．我们特别要求除了单位元外 R 没有任何对称性．因而群中的每一个元素都会将 R 移动到一个不同的位置，称为 gR．所要求的图形 F 是所有图形 gR 的并集．G 的一个元素 x 将 gR 映到 xgR，它也是 F 的一部分．如果 R 充分地随机，G 将是其对称群．正如我们从万花筒所知道的，图形 F 常常是非常引人入胜的．下面是当 G 是正五边形的对称二面体群时，应用这一方法所得的结果．

166



当然，许多图形都会有相同或类似的对称群．尽管如此，根据其对称群对图形进行分类仍是很有意思并具有指导意义的．我们将讨论群的大致的分类，在练习中将会对它们加以改进．

研究离散群的两个主要工具是其平移群及其点群．G 的平移群是满足 $t_a \in G$ 的向量 a 的集合．因为 $t_a t_b = t_{a+b}$ 且 $t_{-a} = t_a^{-1}$，所以这是向量加法群的一个子群，我们将它记为 L_G．利用选定的坐标系，可将向量空间等同于$\mathbb{R}^2$．则

【4.2】
$$L_G = \{a \in \mathbb{R}^2 \mid t_a \in G\}.$$

这个群通过同构(2.10)：$a \rightsquigarrow t_a$ 同构于 G 的平移子群 $T \cap G$．因为它是 G 的子群，所以 $T \cap G$ 是离散的：离散群的子群是离散的．如果把这个条件翻译到 L_G 上，我们得到

【4.3】 除了零向量外 L_G 中没有其他长度 $<\varepsilon$ 的向量．

对某个 $\varepsilon > 0$，$\mathbb{R}^{n+}$ 满足条件(4.3)的子群 L 称为$\mathbb{R}^n$ 的离散子群．这里形容词离散是指 L 的元素被固定的距离隔开：

【4.4】 如果两个向量 a，$b \in L$ 满足 $a \neq b$，则 a，b 的距离至少是 ε．

距离是 $b-a$ 的长度，因为 L 是子群，有 $b-a \in L$．

【4.5】命题 $\mathbb{R}^2$ 的每一离散子群具有下列形式之一：

167

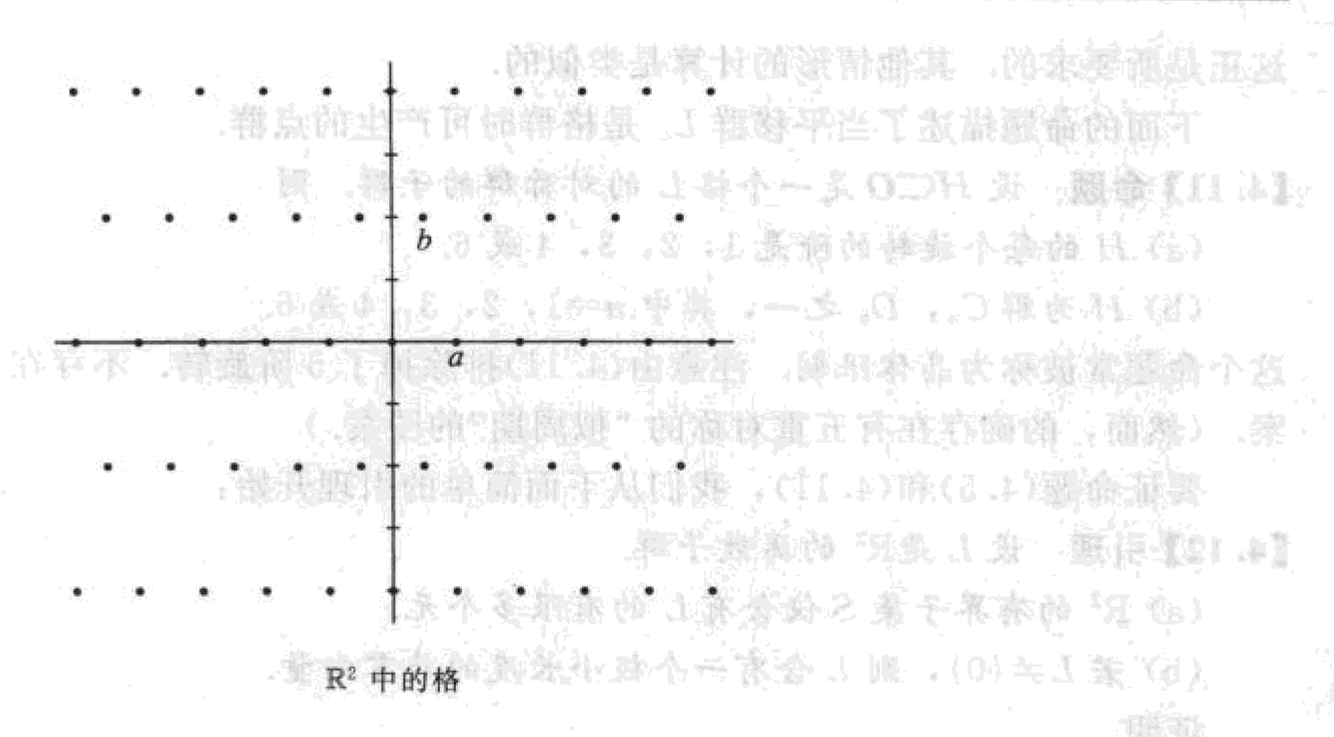
(a) $L = \{0\}$．

(b) L 是一个非零向量 a 生成的加法群：
$$L = \{ma \mid m \in \mathbb{Z}\}.$$

(c) L 由两个线性无关的向量 a，b 生成：
$$L = \{ma + nb \mid m, n \in \mathbb{Z}\}.$$

第三类的群称为平面格，生成元集合(a, b)称为格基．

【4.6】图



$\mathbb{R}^2$ 中的格

我们暂缓命题(4.5)的证明而转到研究离散运动群的第二个工具——它的点群. 回忆存在一个同态 $\varphi: M \longrightarrow \boldsymbol{O}$(2.13)，其核为 T. 如果将这个同态限制到 G，便得到一个同态

【4.7】
$$\varphi|_G: G \longrightarrow \boldsymbol{O}.$$

其核为 $T \cap G$(这是与平移群 L_G 同构的子群). 点群 $\overline{G}$ 是 G 在 $\boldsymbol{O}$ 中的象. 这样，$\overline{G}$ 是 $\boldsymbol{O}$ 的一个子群.

由定义，如果 G 中含有某个形如 $t_a\rho_\theta$ 的元素，则旋转 ρ_θ 属于 $\overline{G}$. 我们在(2.8)已看到 $t_a\rho_\theta$ 是围绕平面上某个点转过角度 θ 的旋转. 因而 $\rho_\theta \in \overline{G}$ 的原象由所有 G 的这样的元素组成，即围绕平面上某个点转过角度 θ 的旋转.

类似地，设 ℓ 表示 $\rho_\theta r$ 的反射轴的直线，如我们前面已注意到的，它与 x 轴的夹角是 $\frac{1}{2}\theta$. 如果 G 中包含某个元素 $t_a\rho_\theta r$，则点群 $\overline{G}$ 包含 $\rho_\theta r$，而 $t_a\rho_\theta r$ 是沿某条与 ℓ 平行的直线的反射或滑动反射. 因而 $\rho_\theta r$ 的原象由 G 中所有这样的元素组成，即它们是沿某条与 ℓ 平行的直线的反射或滑动反射.

因为 G 中没有小运动，这样在点群 $\overline{G}$ 中也没有. 从而 $\overline{G}$ 也是离散的——它是 $\boldsymbol{O}$ 的离散子群. 168

【4.8】命题　*$\boldsymbol{O}$ 的离散子群是有限群.*

我们将这个命题的证明留作练习.

把命题(4.8)和定理(3.4)结合起来，可得下面的结论：

【4.9】推论　*离散群 G 的点群 $\overline{G}$ 为循环群或二面体群.*

下面是一个联系点群与平移群的关键事实：

【4.10】命题　*设 G 是 M 的离散子群，其平移群为 $L=L_G$ 而点群为 $\overline{G}$. $\overline{G}$ 的元素将群 L 映到自身. 换言之，若 $\overline{g} \in \overline{G}$ 而 $a \in L$，则 $\overline{g}(a) \in L$.*

我们可将命题复述为，当 L 被视为平面 $\mathbb{R}^2$ 的点集时，$\overline{G}$ 含于 L 的对称群中. 然而重要的是要注意原来的群 G 不必在 L 上作用.

证明　$a \in L$ 表明 $t_a \in G$. 于是需要证明，如果 $t_a \in G$ 且 $\overline{g} \in \overline{G}$，则 $t_{\overline{g}(a)} \in G$. 由点群的定义，$\overline{g}$ 是群 G 中某个元素 g 的象：$\varphi(g)=\overline{g}$. 我们通过证明 $t_{\overline{g}(a)}$ 是 t_a 由 g 做的共轭来证明命题. 记 $g=t_b\rho$ 或 $t_b\rho r$，其中 $\rho=\rho_\theta$. 则根据不同情形，有 $\overline{g}=\rho$ 或 ρr. 在第一种情形，

$$gt_ag^{-1} = t_b\rho\, t_a\rho^{-1}t_{-b} = t_bt_{\rho(a)}\rho\rho^{-1}t_{-b} = t_{\rho(a)},$$

这正是所要求的. 其他情形的计算是类似的. ■

下面的命题描述了当平移群 L_G 是格群时可产生的点群.

【4.11】命题 设 $H\subset O$ 是一个格 L 的对称群的子群. 则

(a) H 的每个旋转的阶是 1, 2, 3, 4 或 6.

(b) H 为群 C_n, D_n 之一, 其中 $n=1$, 2, 3, 4 或 6.

这个命题常被称为晶体限制. 注意由(4.11)排除掉了 5 阶旋转. 不存在五重旋转对称的墙纸图案. (然而, 的确存在有五重对称的"拟周期"的图案.)

要证命题(4.5)和(4.11), 我们从下面简单的引理开始:

【4.12】引理 设 L 是$\mathbb{R}^2$ 的离散子群.

(a) $\mathbb{R}^2$ 的有界子集 S 仅含有 L 的有限多个元.

169

(b) 若 $L\neq\{0\}$, 则 L 含有一个极小长度的非零向量.

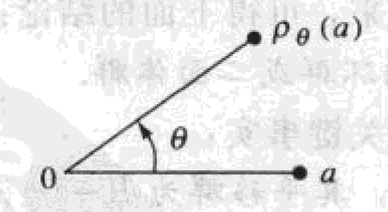
证明

(a) 回顾$\mathbb{R}^n$ 的子集 S 称为有界的, 如果它包含在某个大盒子里, 或者说, 如果 S 的点没有任意大的坐标. 显然, 如果 S 有界, $L\cap S$ 亦有界. 但有界集如果是无限的, 则一定含有互相任意靠近的元素——即其元素不能被固定的正距离 ε 所分离. 而由(4.4), L 不是这样的. 于是 $L\cap S$ 是有限集.

(b) 当我们说非零向量 a 有极小长度, 是指每一非零向量 $v\in L$ 的长度至少是 $|a|$. 我们并不要求向量 a 是唯一确定的. 事实上也无法要求这一点, 因为当 a 有极小长度时, $-a$ 也有极小长度.

假设 $L\neq\{0\}$. 为证一个极小长度的向量存在, 我们设 $b\in L$ 是任意非零向量, 并设 S 是以原点为圆心半径是 $|b|$ 的圆盘. 这个圆盘是有界集, 因而它含有有限多个 L 中的元素, 包括 b 在内. 我们在这有限多个元中找一个有极小长度的非零向量, 它将是所求的最短向量. ■

命题(4.11)的证明 由(3.6), 命题的第二部分由第一部分得到. 要证(a), 设 θ 是 H 中旋转的最小非零角度, 并设 a 是 L 中长度极小的非零向量. 则由于 H 在 L 上作用, $\rho_\theta(a)$亦属于 L; 因此 $b=\rho_\theta(a)-a\in L$. 因为 a 具有极小长度, 故 $|b|\geqslant|a|$. 由此得到 $\theta\geqslant\frac{2\pi}{6}$.



这样 ρ_θ 的阶$\leqslant 6$. 因为这时 $b'=\rho_\theta^2(a)+a$ 比 a 短, $\theta=\frac{2\pi}{5}$也被排除掉:

这就完成了证明. ■

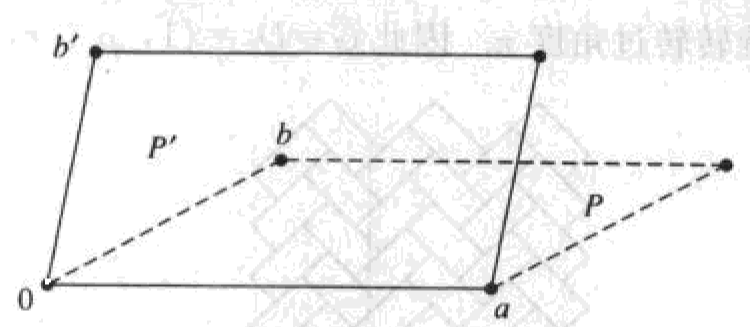
命题(4.5)的证明 设 L 是$\mathbb{R}^2$ 的离散子群. $L=\{0\}$的情形也在列表中. 如果 $L\neq\{0\}$，则存在非零向量 $a\in L$，于是有以下两种可能情形.

170

情形 1：L 中所有向量位于一条过原点的直线 ℓ 之上. 我们重复前面用过多次的一个论证，选择一个长度极小的非零向量 $a\in L$. 我们断言 L 由 a 生成. 设 v 是 L 中的任意元素. 则它是 a 的一个实数倍 $v=ra$，这是因为 $L\subset\ell$. 取 r 的整数部分，记 $r=n+r_0$，其中 n 是整数且 $0\leqslant r_0<1$. 则 $v-na=r_0a$ 的长度小于 a，由于 L 是群，这个元素也属于 L. 从而 $r_0=0$. 这说明 v 是 a 的整数倍，因此属于 a 所生成的子群，这正是要证的.

情形 2：L 的元素不在一条直线上. 则 L 含有两个线性无关的向量 a'，b'. 我们从任意一对线性无关的向量开始，试着用会生成群 L 的向量代替它们. 作为开始，我们用 a'所张成的直线 ℓ 上最短的非零向量 a 代替 a'. 这样，情形 1 的讨论表明子群 $\ell\cap L$ 由 a 生成. 然后考虑顶点为 0，a，b'，$a+b'$的平行四边形 P'：

【4.13】图



因为 P'是有界集，它只包含有限多个 L 的点(4.12). 我们可以搜索这个有限集合并选取一个到直线 ℓ 的距离尽可能短但为正的向量 b. 用这个向量代替 b'. 令 P 为顶点为 0，a，b，$a+b$ 的平行四边形. 我们注意除了其顶点外，P 不含 L 的点. 为此，先注意到 P 中不是顶点的任意格点 c 必属于线段[b，$a+b$]或[0，a]之一. 否则，两个点 c 和 $c-a$ 就比 b 距 ℓ 更近，且这两点之一必位于 P'. 其次，由于 a 是 ℓ 上最短的向量，线段[0，a]被排除在外. 最后，如果有点 c 位于[b，$a+b$]之上，则 $c-b$ 是 L 中位于线段[0，a]之上的点. 证明由下列引理完成.

【4.14】引理 设 a，b 是$\mathbb{R}^2$ 的子群 L 中线性无关的向量. 假设它们张成的平行四边形除了顶点 0，a，b，$a+b$ 外不含 L 中的其他点. 则 L 由 a，b 生成，即

$$L=\{ma+nb\mid m,n\in\mathbb{Z}\}.$$

证明 设 v 是 L 的任意元素. 则由于(a，b)是$\mathbb{R}^2$ 的基，v 是一个线性组合，比如 $v=ra+sb$，其中 r，s 是实数. 取 r，s 的整数部分，记 $r=m+r_0$，$s=n+s_0$，其中 m，n 为整数且 $0\leqslant r_0$，$s_0<1$. 设 $v_0=r_0a+s_0b=v-ma-nb$. 则 v_0 属于平行四边形 P，且 $v_0\in L$. 因而 v_0 为 P 的项点之一，又由于 r_0，$s_0<1$，它必为原点. 这样 $v=ma+nb$. 这就完成了引理和命题(4.5)的证明. ■

171

设 L 是$\mathbb{R}^2$ 的格. 元素 $v\in L$ 称为本原的，如果它不是 L 中另一个向量的整数倍. 前面的证明实际上证明了下面的结论：

【4.15】推论 设 L 是格，且设 v 是 L 的本原元. 则存在 L 的元素 $w\in L$ 使得集合(v，w)是一个格基.

现在我们回到离散运动群 $G\subset M$，并考虑根据其平移群 L_G 的结构的大致分类. 如果

L_G 是平凡群，则由 G 到其点群的同态是双射且 G 是有限群．我们已在第三节验证了这种情形．

使得 L_G 为无限循环群的离散群 G 是如图(1.3)所示的带状图案的对称群．这些群的分类留作练习．

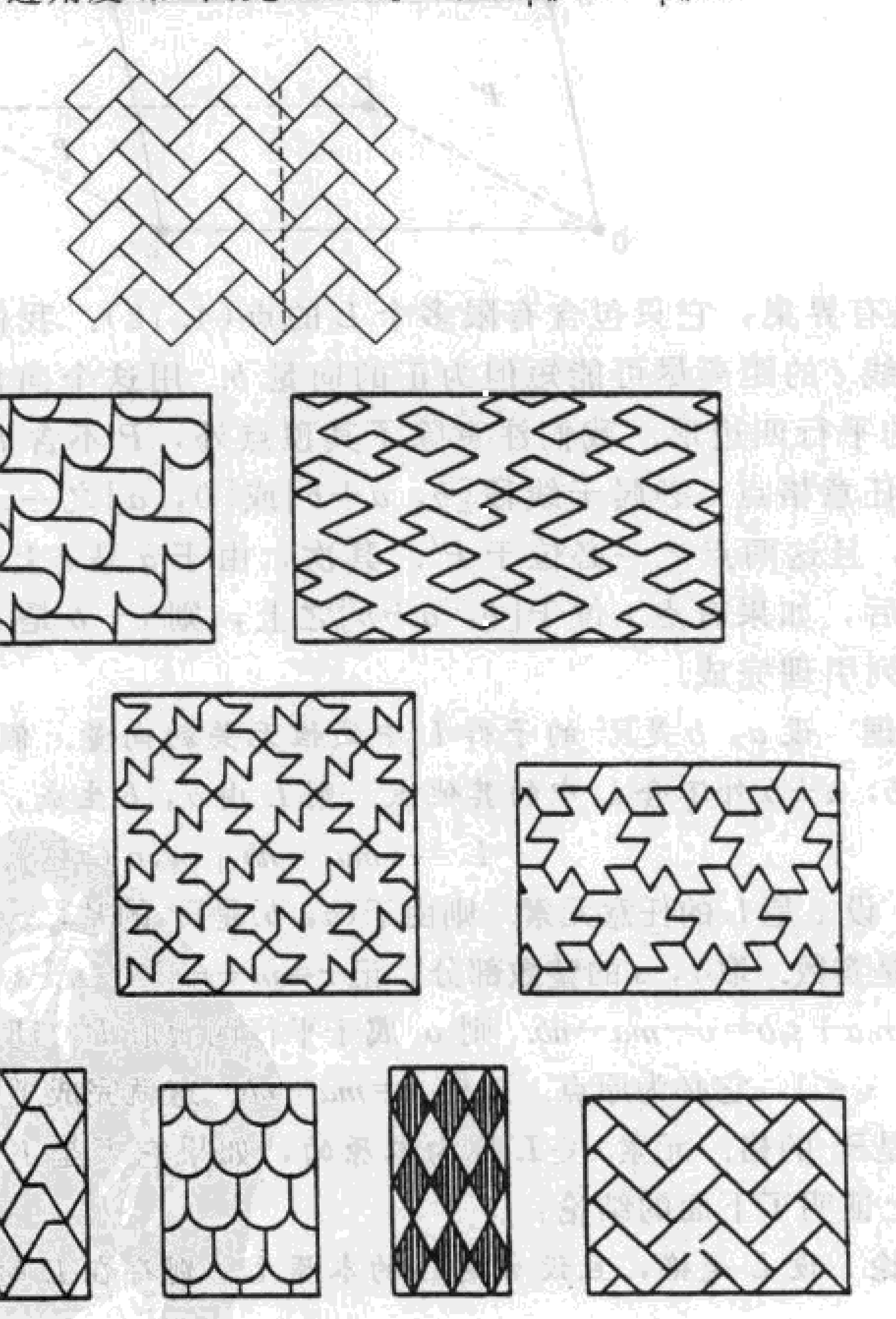
如果 L_G 是格，则 G 称为*二维晶体群*或*格群*．这些群是墙纸图案和二维晶体的对称群．

任意墙纸图案在两个不同的方向上重复，这一事实反映了其对称群总是包含两个无关平移，这说明 L_G 是一个格．它还可以包含其他元素——旋转、反射或滑动——但晶体条件限制了其可能性，而使得晶体群分成17类．分类不仅考虑群的内部结构，而且考虑每个群元素所代表的运动类型．不同类型的对称的代表图案见图(4.16)．

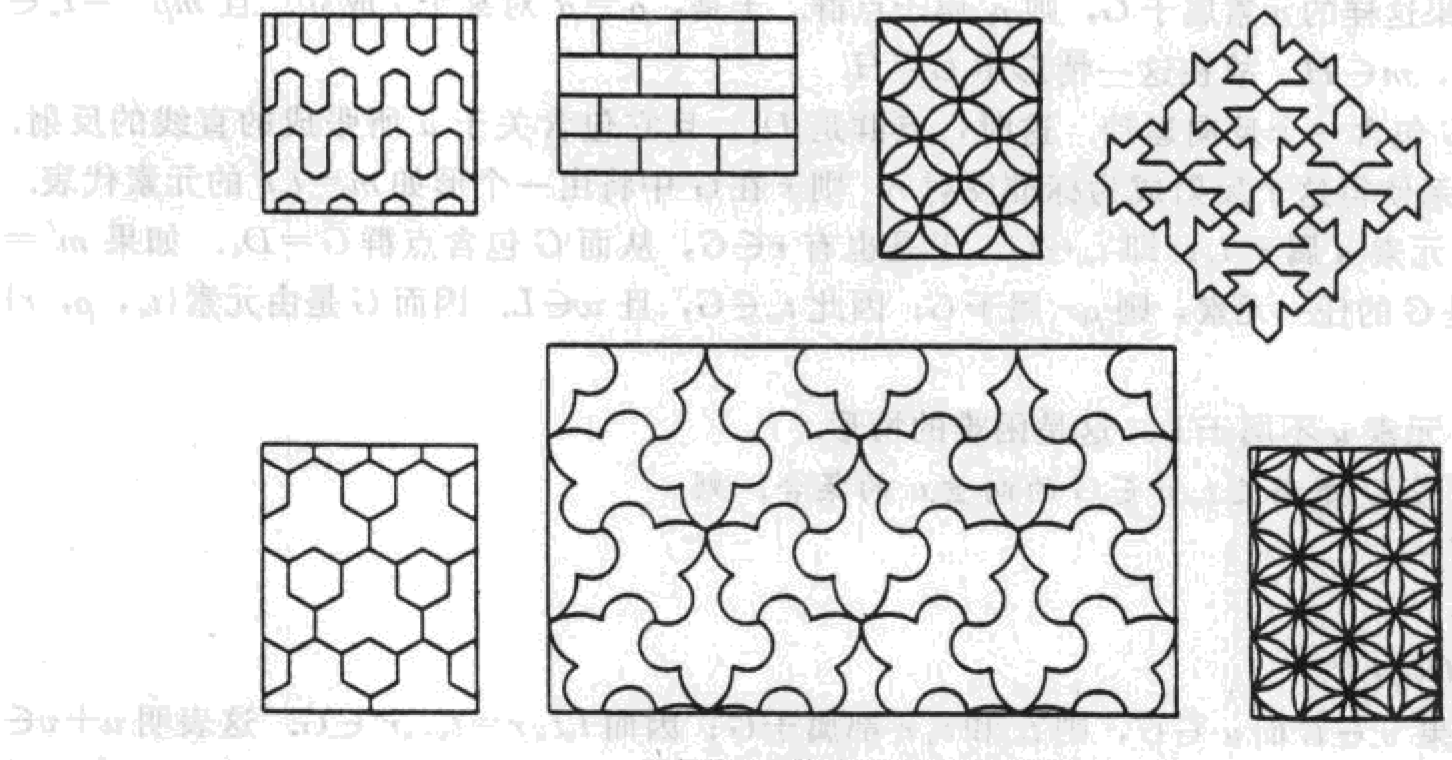
命题(4.11)对确定晶体群的点群非常有用．例如，下面所示的砖状图案有一个围绕这些砖的中心转过角度 π 的旋转对称．所有这些旋转代表点群 $\overline{G}$ 中的同一个元素 ρ_π．图案也有沿所画虚线的滑动对称．因而点群包含一个反射．由命题(4.11)，$\overline{G}$ 是二面体群．另一方面，容易看出对称群中仅有的非平凡旋转转过角度 π．因此 $\overline{G}=D_2=\{1, \rho_\pi, r, \rho_\pi r\}$．

172

【4.16】图



17个平面晶体群的图案范例



17 个平面晶体群的图案范例(续)

173

点群 $\overline{G}$ 和平移群 L_G 没有完全刻画群 G. $\overline{G}$ 中的反射不必是 G 中一个反射的象这一事实使事情变得复杂——如前面砖形图案所示，它在 G 中可能只由一个滑动代表.

作为二维晶体群分类方法的范例，我们将刻画点群含有转过角度$\frac{\pi}{2}$的旋转 ρ 的二维晶体群. 根据命题(4.11)，点群将是 C_4 或 D_4. 因为 G 中代表 ρ 的任意元素亦是围绕某个点 p 转过角度$\frac{\pi}{2}$的旋转，所以可取 p 为原点. 这样 ρ 也可以看作是 G 中的元素.

【4.17】命题 *设 G 是格群，其点群含有转过角度$\frac{\pi}{2}$的旋转 ρ. 选择坐标系使得原点是 G 中转过角度$\frac{\pi}{2}$的旋转所绕的点. 设 a 是 $L=L_G$ 中的最短向量，令 $b=\rho(a)$，并令 $c=\frac{1}{2}(a+b)$. 用 r 表示关于由 a 张成的直线的反射. 则 G 由下列集合之一生成：$\{t_a, \rho\}$，$\{t_a, \rho, r\}$，$\{t_a, \rho, t_c r\}$. 因而存在三个这样的群.*

证明 首先注意到 L 是方格，它由 a，b 生成. 因为，由假设 a 属于 L，而命题(4.10)断言$b=\rho(a)$也属于 L. 这两个向量生成 L 的一个方子格 L'. 如果 $L\neq L'$，则根据引理(4.14)，存在元素 $w\in L$，它位于顶点为 0，a，b，$a+b$ 的正方形中，且它不是这些顶点之一. 但任何一个这样的向量至少到一个顶点 v 的距离小于 $|a|$，且差 $w-v$ 属于 L 且其长度比 a 短，这与 a 的选择矛盾. 这样 $L=L'$，正是我们所断言的.

既然 t_a 和ρ 都属于G，且 $\rho t_a \rho^{-1}=t_b$(2.5)，因而 G 由集合$\{t_a, \rho\}$生成的子群 H 包含 t_a 和 t_b. 因此对每个 $w\in L$，它也包含 t_w. 这个群的元素为积 $t_w\rho^i$：

$$H = \{t_w\rho^i \mid w \in L, 0 \leqslant i \leqslant 3\}.$$

这是我们的群之一，现在考虑 G 所可能包含的别的元素.

情形 1：G 的每个元素保向. 在这种情形中，G 的点群是 C_4. G 的每一个元素具有$m=t_u\rho_\theta$

的形式，且如果这样的元素属于 G，则 ρ_θ 属于点群．于是，$\rho_\theta=\rho^i$ 对某个 i 成立．且 $m\rho^{-i}=t_u\in G$．因而 $u\in L$，$m\in H$．故在这一情形中 $G=H$．

情形 2：G 包含一个反向运动．这时，点群是 D_4，且它包含关于 a 所张成的直线的反射．我们选择坐标系使得这个反射成为标准反射 r．则 r 在 G 中将由一个形如 $m=t_u r$ 的元素代表．

情形 2a：元素 u 属于 L；即 $t_u\in G$．于是也有 $r\in G$，从而 G 包含点群 $\overline{G}=D_4$．如果 $m'=$ 174 $t_w\rho_\theta$ 或 $t_w\rho_\theta r$ 是 G 的任一元素，则 $\rho_\theta r$ 属于 G；因此 $t_w\in G$，且 $w\in L$．因而 G 是由元素 $\{t_a,\ \rho,\ r\}$ 生成的群．

情形 2b：元素 u 不属于 L．这是困难的情形．

【4.18】引理　*设 U 是满足 $t_u r\in G$ 的向量 u 的集合．则*

(a) $L+U=U$.

(b) $\rho U=U$.

(c) $U+rU\subset L$.

证明　如果 $v\in L$ 而 $u\in U$，则 t_v 和 $t_u r$ 都属于 G；因而 $t_v t_u r=t_{v+u}r\in G$．这表明 $u+v\in U$，从而证明了(a)．其次，设 $u\in U$．则 $\rho t_u r\rho=t_{\rho u}\rho r\rho=t_{\rho u}r\in G$．这表明 $\rho u\in U$，从而证明了(b)．最后，若 u，$v\in U$，则 $t_u r t_v r=t_{u+rv}\in G$；因而 $u+rv\in L$，这证明了(c)． ■

引理中(a)使我们能选择 $u\in U$，它位于顶点为 0，a，b，$a+b$ 的正方形中，但不在线段 $[a,\ a+b]$ 和 $[b,\ a+b]$ 上．用基 $(a,\ b)$ 写出 u，比如 $u=xa+yb$，其中 $0\leqslant x$，$y<1$．则 $u+ru=2xa$．因为由(4.18c)，$u+ru\in L$，所以 x 可能的值为 0，$\frac{1}{2}$．其次，$\rho u+a=(1-y)a+xb$ 也属于该正方形，同样的推理表明 y 是 0 或 $\frac{1}{2}$．这样 u 的三种可能为 $\frac{1}{2}a$，$\frac{1}{2}b$ 和 $\frac{1}{2}(a+b)=c$．但如果 $u=\frac{1}{2}a$，则 $\rho u=\frac{1}{2}b$ 且 $ru=u=\frac{1}{2}a$．于是 $c=\frac{1}{2}(a+b)\in L$(4.18b，c)．因为 c 比 a 短，这是不可能的．类似地，$u=\frac{1}{2}b$ 的情形也是不可能的．剩下的仅有的情形是 $u=c$，这表明群 G 由 $\{t_a,\ \rho,\ t_c r\}$ 生成． ■

第五节　抽象对称：群作用

对称的概念可以应用到除几何图形之外的其他对象上．例如，复共轭 $(a+bi)\rightsquigarrow(a-bi)$ 可以认为是复数的对称．它与 $\mathbb{C}$ 的大多数结构相容：如果用 $\bar{\alpha}$ 表示 α 的复共轭，则 $\overline{\alpha+\beta}=\bar{\alpha}+\bar{\beta}$，$\overline{\alpha\beta}=\bar{\alpha}\bar{\beta}$．由于与加法和乘法相容，共轭称为域 $\mathbb{C}$ 的自同构．当然，这个对称只是复平面关于其实轴的双边对称，但是，它是自同构这一说法涉及其代数结构．

另一个抽象"双边"对称的例子是 3 阶循环群．在第二章第三节我们看到，这个群有一个自同构 φ，它交换 H 中不等于单位元的两个元素．

一个群 H(或任何其他数学结构 H)的自同构的集合构成一个群 $\mathrm{Aut}H$，合成法则为映射的合成．在下面的意义下每个自同构都可以看作是 H 的对称：它是与 H 的结构相容的 H 中元素 175 的一个置换．但在这种情形下，用来取代具有刚性形状的几何图形的结构是群法则．3 阶循环群的自同构群包含两个元素：恒等映射和映射 φ．

因此，自同构和对称这两个词的意义或多或少是相同的，只是自同构用于描述保持某个代

数结构的集合的置换，而对称常指保持几何结构的置换.

这些例子都是群在集合上作用这个更一般的概念的特殊情形. 假设给定一个群 G 和一个集合 S. G 在 S 上的一个作用是组合元素 $g\in G$ 和 $s\in S$ 而得到 S 的元素 gs 的法则. 换言之，它是一个合成法则，一个映射 $G\times S\longrightarrow S$，一般把它写作乘法：

$$g,s \rightsquigarrow gs.$$

该法则需要满足下列公理：

【5.1】

(a) 对所有 s，有 $1s=s$(1 是 G 的单位元).

(b) 结合律：对所有 g，$g'\in G$ 和 $s\in S$，有 $(gg')s=g(g's)$.

具有 G 的作用的一个集合 S 通常称为一个 G-集合. 实际上这应该叫做一个*左*作用，因为 G 的元素是从左边乘.

这一概念的例子在许多地方都能找到. 例如，设 $G=M$ 是平面的所有刚体运动的群. 则 M 在平面上的点集上作用，在平面上的直线集合上作用，在平面上的三角形的集合上作用，等等. 设 G 是 2 阶循环群$\{1, r\}$，其中 $r^2=1$. 则 G 通过法则 $r\alpha=\bar{\alpha}$ 在复数集合 S 上作用. 在所给的例子里，公理(5.1)成立这一事实通常是很清楚的.

把这样的合成法则称为作用的原因在于：如果固定一个元素 $g\in G$ 而让元素 $s\in S$ 变动，则用 g *左乘*定义一个 S 到其自身的映射，记这个映射为 m_g. 这样

【5.2】

$$m_g: S\longrightarrow S$$

由

$$m_g(s)=gs$$

定义. 这个映射描述了元素 g 在 S 上作用的方式. 注意 m_g 是 S 的一个*置换*；即它是一一映射. 因为公理已指出它具有双边逆

$$m_{g^{-1}}=\text{用 } g^{-1}\text{ 乘}:$$

$m_{g^{-1}}(m_g(s))=g^{-1}(gs)=(g^{-1}g)s=1s=s$. 交换 g 与 g^{-1} 也表明有 $m_g(m_{g^{-1}}(s))=s$.　　176

研究一个群 G 在集合 S 上的作用，主要是将集合分解成轨道. 设 s 是 S 的一个元素. s 在 S 中的*轨道*是集合

【5.3】

$$O_s=\{s'\in S\mid \text{对某个 } g\in G, s'\in gs\}.$$

它是 S 的一个子集.(轨道常记作 $Gs=\{gs\mid g\in G\}$，类似于陪集的记号[第二章(6.1)]. 不用这个记号是因为 Gs 看起来太像我们将要引入的稳定子的记号.)如果把 G 中的元素想象为置换在 S 上的作用，则 O_s 是 s 在不同的置换 m_g 之下的象的集合. 这样，如果 $G=M$ 是运动群而 S 是平面上三角形的集合，则一个给定三角形 Δ 的轨道 O_Δ 是所有与 Δ 全等的三角形的集合. 轨道的另一个例子是我们在证明平面上有限群作用的不动点的存在性的证明(3.1)中所引入的那个.

群作用的轨道是以下关系的等价类.

【5.4】 $s\sim s'$，如果对某个 $g\in G$ 有 $s'=gs$.

容易证明这是等价关系，我们将其省去，而是作一个与第二章第六节引入陪集时的类似的验证. 轨道作为等价类给出了集合 S 的划分：

【5.5】S 是轨道的不相交的并.

群 G 通过在每条轨道上独立地作用而对 S 作用. 换言之，一个元素 $g\in G$ 置换每一条轨道中的元素，而不将一条轨道中的元素映到另一条轨道. 例如，平面上的三角形的集合可以划分为全等类，也就是 M 的作用的轨道. 一个运动 m 分别置换每一个全等类. 注意元素 s 和 gs 的轨道是相同的.

若 S 仅由一条轨道构成，我们称 G 在 S 上可迁地作用. 这时 S 的每一个元素可通过群中的某个元素映为任意其他的元素. 这样图(1.7)的对称群可迁地作用于其"腿"的集合. 平面刚体运动群 M 可迁地作用于平面上的点的集合，同时也可迁地作用于平面上的直线的集合. 但它不是可迁地作用于平面上的三角形的集合.

元素 $s\in S$ 的稳定子是 G 中保持 s 不动的元素的子群 G_s：

【5.6】
$$G_s=\{g\in G\mid gs=s\}.$$

这显然是一个子群. 就像群同态 $\varphi:G\longrightarrow G'$ 的核告诉我们什么时候两个元素有同样的象一样，也就是说，如果 $x^{-1}y\in\ker\varphi$[第二章(5.13)]，我们可用稳定于 G_s 的语言描述什么时候两个元素 x，$y\in G$ 用相同的方式作用于元素 s：

177

【5.7】$xs=ys$ 当且仅当 $x^{-1}y\in G_s$.

这是因为 $xs=ys$ 蕴涵 $s=x^{-1}ys$，反之亦然.

作为非平凡稳定子的例子，考虑刚体运动群 M 在平面上点的集合的作用. 原点的稳定子是正交算子的子群 $\boldsymbol{O}$.

或者，若 S 是平面上三角形的集合且 Δ 是其中一个特定的等边三角形，则 Δ 的稳定子是它的对称群，也就是 M 的一个同构于 D_3 的子群(见(3.4)). 注意我们说一个运动 m 稳定一个三角形 Δ，不是指 m 保持 Δ 的点不动. 保持三角形每个点不动的运动只能是恒等映射. 我们指的是在对三角形集合进行置换时，运动将 Δ 映到其自身. 搞清楚这一区别是很重要的.

第六节 对陪集的作用

设 H 是群 G 的一个子群. 在第二章第六节我们看到，左陪集 $aH=\{ah\mid h\in H\}$ 构成群的一个划分[第二章(6.3)]. 我们称左陪集的集合为陪集空间，并常将它记为 G/H，当子群为正规子群时沿用与商群相同的记号.

观察这样一个基本事实：尽管除了 H 是正规子群以外，G/H 不是群，然而，G 可以以一种自然的方式在陪集空间 G/H 上作用. 作用是相当明显的：设 g 是 G 的元素，并设 C 是一个陪集. 则 gC 定义为陪集

【6.1】
$$gC=\{gc\mid c\in C\}.$$

这样，如果 $C=aH$，则 gC 是陪集 gaH. 显然，作用满足公理(5.1).

注意，群 G 可迁地作用在 G/H 上，这是因为 G/H 是陪集 $1H=H$ 的轨道. 陪集 $1H$ 的稳定子是子群 $H\subset G$. 再一次提请注意区别：由元素 $h\in H$ 乘在陪集 $1H$ 的元素上的作用并不是平凡的，但它将陪集映到自身.

要理解在陪集上的作用，应该仔细地推敲一下下面的例子. 设 G 是等边三角形的对称群 D_3. 如在(3.6)中一样，可以用满足关系 $x^3=1$，$y^2=1$，$yx=x^2y$ 的生成元 x，y 来描述这个

群. 设 $H=\{1, y\}$. 这是一个二阶子群. 其陪集为

【6.2】 $C_1 = H = \{1, y\}$， $C_2 = \{x, xy\}$， $C_3 = \{x^2, x^2 y\}$，

并且 G 在 $G/H=\{C_1, C_2, C_3\}$ 上作用. 因而，如(5.2)一样，每个元素 $g\in G$ 确定一个 $\{C_1, C_2, C_3\}$ 的置换. 元素 x，y 的作用如下：

【6.3】图

m_x: 1 → 2 → 3 → 1, m_y: 1 固定, 2 ⇄ 3.

178

事实上，G 的六个元素产生三个元素的所有六个置换，因而映射

$$G \longrightarrow S_3 \approx \mathrm{Perm}(G/H)$$
$$g \rightsquigarrow m_g$$

是一个同构. 这样，二面体群 $G=D_3$ 同构于对称群 S_3. 这一点我们已经知道.

下面的命题将任意群作用与它在陪集上的作用联系起来：

【6.4】命题 设 S 是一个 G-集合，并设 s 是 S 的一个元素. 设 H 是 s 的稳定子，并设 O_s 是 s 的轨道. 则存在一个自然的双射

$$G/H \xrightarrow{\varphi} O_s,$$

它由

$$aH \rightsquigarrow as$$

定义.

这个映射在下面的意义下与 G 的作用相容：对每一个陪集 C 及每个元素 $g\in G$，有 $\varphi(gC)=g\varphi(C)$.

命题告诉我们每个群作用可以用它在陪集上的作用来描述. 例如，设 $S=\{v_1, v_2, v_3\}$ 为一个等边三角形的顶点的集合，并设 G 是其对称群，如上面所表出. 元素 y 是使三角形一个顶点(比如 v_1)固定不动的反射. 这个顶点的稳定子是 $H=\{1, y\}$，其轨道为 S. 用适当的下标，通过映射 $C_i \rightsquigarrow v_i$ 可将陪集(6.2)映到 S.

命题(6.4)的证明 显然，如果映射 φ 存在，则它与群的作用是相容的. 究竟法则 $gH \rightsquigarrow gs$ 能否定义一个映射并不清楚. 因为许多符号 gH 代表的是同一个陪集，我们必须证明，如果 a，b 是群的元素且如果 $aH=bH$，则也有 $as=bs$. 这是成立的，因为 $aH=bH$ 当且仅当对某个 $h\in H$ 有 $b=ah$[第二章(6.5)]. 而当 $b=ah$ 时，则因为 h 使 s 不动，故 $bs=ahs=as$. 其次，s 的轨道由元素 gs 组成，且 φ 将 gH 映到 gs. 这样 φ 将 G/H 映到 O_s 上且 φ 是满射. 最后我们证明 φ 是单射. 设 aH 与 bH 有相同的象：$as=bs$. 则 $s=a^{-1}bs$. 因为 H 定义为 s 的稳定子，这蕴涵 $a^{-1}b=h\in H$. 这样 $b=ah\in aH$，从而 $aH=bH$. 这就完成了证明. ■

【6.5】命题 设 S 是一个 G-集合，并设 $s\in S$. 设 s' 是 s 的轨道中的一个元素，比如 $s'=as$. 则

(a) G 中满足 $gs=s'$ 的元素 g 的集合是左陪集

$$aG_s = \{g\in G \mid 存在\ h\in G_s, 使得\ g=ah\}.$$

179

(b) s' 的稳定子是 s 的稳定子的一个共轭子群：

$$G_{s'} = aG_s a^{-1} = \{g\in G \mid 存在\ h\in G_s, 使得\ g=aha^{-1}\}.$$

我们省去证明.

作为例子，我们对运动群的作用重新计算平面上点 p 的稳定子．在前面(2.11b)中已经计算过这个群．我们有 $p=t_p(0)$，而原点的稳定子是正交群 $\mathbf{O}$．这样由(6.5b)，

$$G_p = t_p\,\mathbf{O}\,t_p^{-1} = t_p\,\mathbf{O}\,t_{-p} = \{m \in M \mid m = t_p\rho_\theta t_{-p} \text{ 或 } m = t_p\rho_\theta r\, t_{-p}\}.$$

另一方面，我们知道 G_p 由绕点 p 的旋转与反射组成．这些都是使 p 不动的运动．因而 $t_p\,\mathbf{O}\,t_p^{-1}$ 由这些元素组成．这与(2.11)是一致的．

第七节　计数公式

设 H 是 G 的子群．我们由第二章(6.9)已知，H 在 G 中的所有陪集有同样数量的元素：$|H|=|aH|$．因为 G 是互不重迭的陪集的并，且陪集的个数是子群的指标，(将其记为$[G:H]$或 $|G/H|$)我们有关于群 G 的阶的基本公式(第二章(6.10))：

【7.1】
$$|G|=|H||G/H|.$$

现在设 S 是 G 集合．我们可以将命题(6.4)和(7.1)合起来得到下面的命题：

【7.2】命题　计数公式：设 $s\in S$．则

$$(G\text{ 的阶}) = (\text{稳定子的阶})(\text{轨道的阶}).$$
$$|G|=|G_s||O_s|.$$

等价地，轨道的阶等于稳定子的指标：

$$|O_s|=[G:G_s].$$

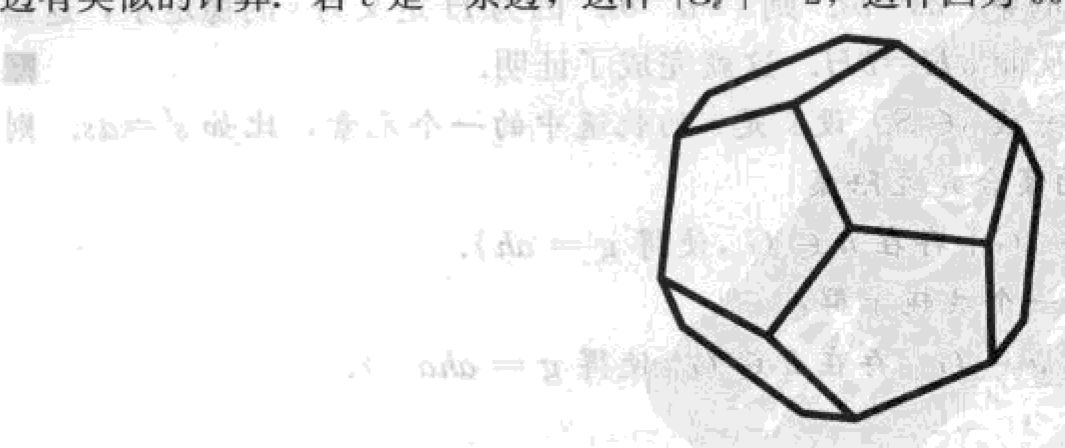
对每个 $s\in S$ 都有一个这样的等式．作为其推论，轨道的阶整除群的阶．

一个更初等的公式利用 S 划分成轨道对其元素的计数．将组成 S 的不同轨道以某种方式标号，比如 $O_1,\cdots,O_k$．则

【7.3】
$$|S|=|O_1|+|O_2|+\cdots+|O_k|.$$

180 这个简单的公式有着大量的应用．

【7.4】例　考虑正十二面体 D 的保向对称群 G．由第四章第五节的讨论可知这些对称都是旋转．把它们正确地数出来是有窍门的．考虑 G 在 D 的面的集合 S 上的作用．面 s 的稳定子是围绕过 s 的中心的垂线转过角度$\frac{2\pi}{5}$的倍数的旋转群．从而 G_s 的阶为5．有12个面，且 G 在它们上可迁地作用．这样 $|G|=5\cdot 12=60$．或者，G 在 D 的顶点 v 上可迁地作用．包括1共有3个旋转使一个顶点不动，因而 $|G_v|=3$．共有20个顶点；因而 $|G|=3\cdot 20=60$，这验证了我们的结果．对于边有类似的计算．若 e 是一条边，这样 $|G_e|=2$，这样因为 $60=2\cdot 30$，正十二面体有30条边．



遵循一般原则，我们应研究群 G 的作用在一个子群上的限制. 假设 G 在一个集合 S 上作用，并设 H 是 G 的子群. 我们可限制作用，得到 H 在 S 上的作用. 这样得到更多的数量关系.

显然，一个元素 s 的 H-轨道包含在其 G-轨道中. 因此可取单独一条 G-轨道并将其关于 H-轨道分解. 我们对这些 H-轨道计数，得到另外一个公式. 例如，设 S 是正十二面体的面的集合，而 H 是某个给定面的稳定子. 则 H 也使与 s 相对的面不变，所以有两条阶为 1 的 H-轨道. 其他面组成两条阶为 5 的轨道. 这时，(7.3)成为：

$$12 = 1 + 1 + 5 + 5.$$

或者假设 S 是面的集合，K 是一个顶点的稳定子. 则 K 不能使任何面不动，因而每一条 K-轨道的阶皆为 3：

$$12 = 3 + 3 + 3 + 3.$$

这些关系给出将一个群 G 的几个子群联系起来的一种方式.

我们在 G-集合是子群的陪集空间这一情形下用这一方法的一个简单应用来结束这一节：

【7.5】命题　*设 H 和 K 是群 G 的子群. 则 $H\cap K$ 在 H 中的指标最多等于 K 在 G 中的指标：*

$$[H:H\cap K]\leqslant[G:K].$$

181

证明　为了避免混乱，我们记陪集空间 G/K 为 S，记陪集 $1K$ 为 s. 则 $|S|=[G:K]$. 正如我们所看到的，s 的稳定子是子群 K. 将 G 的作用限制到子群 H 上，并 S 分解成为 H-轨道. 对于这个限制作用，s 的稳定子显然是 $H\cap K$. 除了它是 S 的子集，我们并不了解 s 的 H-轨道 O. 应用命题(7.2)可知 $|O|=[H:H\cap K]$. 于是 $[H:H\cap K]=|O|\leqslant|S|=[G:K]$，这正是需要证明的. ■

第八节　置换表示

由定义，对称群 S_n 在集合 $S=\{\mathbf{1},\cdots,\mathbf{n}\}$ 上作用. 群 G 的**置换表示**是一个同态

【8.1】
$$\varphi:G\longrightarrow S_n.$$

给定任意一个这样的表示，通过令 m_g 为置换 $\varphi(g)$(5.2)，可以得到 G 在 $S=\{\mathbf{1},\cdots,\mathbf{n}\}$ 上的作用. 事实上，群 G 在 $\{\mathbf{1},\cdots,\mathbf{n}\}$ 上的作用以双射的方式对应于置换表示.

更一般地，设 S 为任一集合，用 $\mathrm{Perm}(S)$ 表示其置换群. 设 G 是一个群.

【8.2】命题　*存在双射对应*

$$\begin{bmatrix} G\text{在}S \\ \text{上的作用} \end{bmatrix} \leftrightarrow \begin{bmatrix} \text{同态} \\ G\longrightarrow \mathrm{Perm}(S) \end{bmatrix},$$

它以这样的方式定义：给定一个作用，用法则 $\varphi(g)=m_g$ 定义 $\varphi:G\longrightarrow \mathrm{Perm}(S)$，其中 m_g 是用 g 乘(5.2).

我们证明 φ 是同态，而将(8.2)的其余部分留作练习. 在第五节中我们已注意到 m_g 是置换. 因而由上面的定义，$\varphi(g)\in \mathrm{Perm}(S)$. 同态的公理是 $\varphi(xy)=\varphi(x)\varphi(y)$ 或 $m_{xy}=m_xm_y$，其中乘积是置换的合成. 因而要证明 $m_{xy}(s)=m_x(m_y(s))$ 对每个 $s\in S$ 成立. 由定义(5.2)，$m_{xy}(s)=(xy)s$ 而 $m_x(m_y(s))=x(ys)$. 群作用的结合律(5.1b)表明 $(xy)s=x(ys)$，这正是所

需要证明的.

在第六节中由 D_3 在 H 的陪集上的作用(6.2)得到的同构 $D_3 \longrightarrow S_3$ 是置换表示的一个特例. 但是一个同态不必是单射或满射. 若 $\varphi: G \longrightarrow \mathrm{Perm}(S)$ 碰巧为单射，我们称对应的作用为忠实的. 因此要成为忠实的，作用必需具有下列性质：除非 $g=1$，否则 $m_g \neq$ 恒等映射，或者说

如果对每个 $g \in S$，$gs=s$ 成立，则 $g=1$.

运动群 M 对平面上等边三角形的集合的作用是忠实的，因为恒等映射是仅有的使所有三角形不变的运动.

182

本节余下的部分包含了置换表示的一些应用.

【8.3】命题 系数模 2 的可逆矩阵的群 $GL_2(\mathbb{F}_2)$ 同构于对称群 S_3.

证明 用 F 表示域$\mathbb{F}_2$，用 G 表示群 $GL_2(\mathbb{F}_2)$. 我们在前面[第三章(2.10)]列出了 G 的六个元素. 设 $V=F^2$ 是列向量空间. 这个空间由下面四个向量构成：$V=\{0, e_1, e_2, e_1+e_2\}$. 群 G 在 V 上的作用使 0 不动，因而它在三个非零向量的集合上作用，这个集合构成一条轨道. 这给出一个置换表示 $\varphi: G \longrightarrow S_3$. e_1 在和一个矩阵 $P \in G$ 乘积下的象是 P 的第一列，同样，e_2 的象是 P 的第二列. 因而除非 P 本身是单位矩阵，否则它不可能在这两个元素上平凡地作用. 这表明 G 的作用是忠实的，因而映射 φ 是个单射. 因为两个群的阶都是 6，所以 φ 是同构. ■

【8.4】命题 设 c_g 表示 g 的共轭，映射 $c_g(x)=gxg^{-1}$. 由法则 $g \rightsquigarrow c_g$ 定义的由对称群 S_3 到其自同构群的映射是一一映射.

证明 设 A 表示 S_3 的自同构群. 由第二章(3.4)可知 c_g 是一个自同构. 而且 $c_{gh}=c_g c_h$，这是因为对所有 x，$c_{gh}(x)=(gh)x(gh)^{-1}=ghxh^{-1}g^{-1}=c_g(c_h(x))$. 这表明 f 是一个同态. 而用 g 共轭是恒等映射当且仅当 g 属于群的中心. S_3 的中心是平凡的，因而 f 是单射.

为了证明 f 是满射，我们来看 A 的置换表示. 群 A 以明显的方式在集合 S_3 上作用；即若 α 是自同构而 $s \in S_3$，则 $\alpha s=\alpha(s)$. S_3 中不同阶的元素将属于这个作用下的不同的轨道. 因而 A 在 S_3 的 2 阶元素的子集上作用. 这个集合含有三个元素$\{y, xy, x^2y\}$. 如果一个自同 α 构使 xy 和 y 都不动，则它亦使其积 $xyy=x$ 不动. 因为 x，y 生成 S_3，仅有的这样的自同构为恒等映射. 这说明 A 在$\{y, xy, x^2y\}$上的作用是忠实的，并且相应的置换表示 $A \longrightarrow \mathrm{Perm}\{y, xy, x^2y\}$是单射. 因此 A 的阶最多是 6. 因为 f 是单射而 S_3 的阶是 6，从而 f 是一一映射. ■

【8.5】命题 p 阶循环群的自同构群同构于$\mathbb{F}_p$ 的非零元素的乘法群$\mathbb{F}_p^{\times}$.

证明 这里的方法是使用加法群$\mathbb{F}_p^{+}$ 作为 p 阶循环群的模型. 它由元素 1 生成. 我们将乘法群$\mathbb{F}_p^{\times}$ 记为G. 则 G 通过左乘对$\mathbb{F}_p^{+}$ 作用，这一作用定义了一个到 p 个元素集$\mathbb{F}_p$ 的置换群的单同态 $\varphi: G \longrightarrow \mathrm{Perm}(\mathbb{F}p)$.

183

其次，自同构群 $A=\mathrm{Aut}(\mathbb{F}_p^{+})$是 $\mathrm{Perm}(\mathbb{F}_p)$的子群. 分配律表明用元素 $a \in \mathbb{F}_p^{\times}$ 左乘是$\mathbb{F}_p^{+}$ 的同构. 它是双射，并且 $a(x+y)=ax+ay$. 因而映射 $\varphi: G \longrightarrow \mathrm{Perm}(\mathbb{F}_p^{+})$的象包含在子群 A 中. 最后，$\mathbb{F}_p^{+}$ 的自同构由它将生成元 1 映到哪儿来确定，而 1 的象不能为 0. 利用 G 的作用，可将 1 映到任意非零元. 因而 φ 是 G 到 A 的满射. 由于 φ 同时是单射和满射，因而它是一个同构. ■

第九节　旋转群的有限子群

本节我们应用计数公式对第四章(5.4)定义的旋转群 SO_3 的有限子群进行分类．如同有限平面运动群一样，SO_3 中只有很少几个有限子群，且它们全部都是熟悉的图形的对称群．

【9.1】定理　*SO_3 的有限子群是下列之一：*

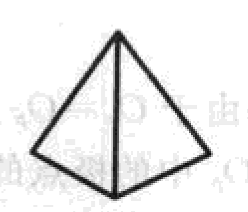
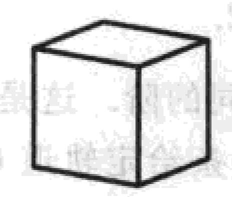
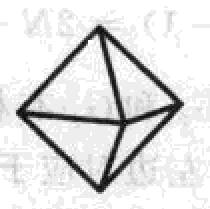
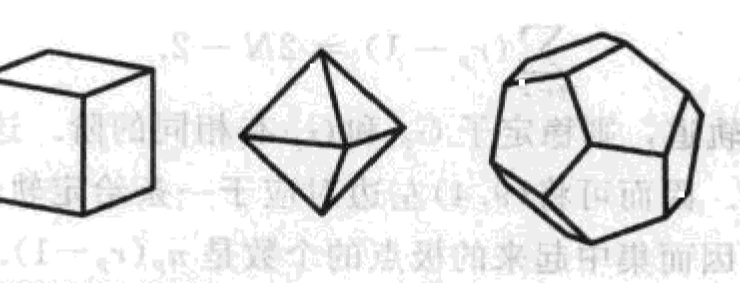
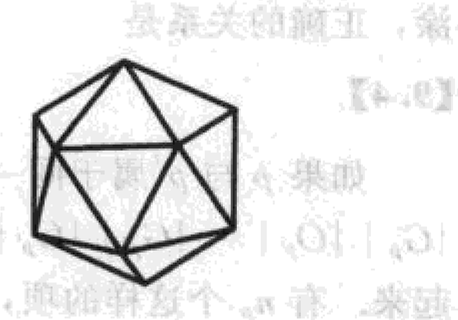
C_k：绕一条直线转过角度 $\frac{2\pi}{k}$ 的倍数的旋转的循环群；

D_k：正 k 边形的对称的二面体群(3.4)；

T：将正四面体映为自身的十二个旋转的四面体群；

O：立方体或正八面体旋转的 24 阶八面体群；

I：正十二面体或正二十面体的 60 个旋转的二十面体群：

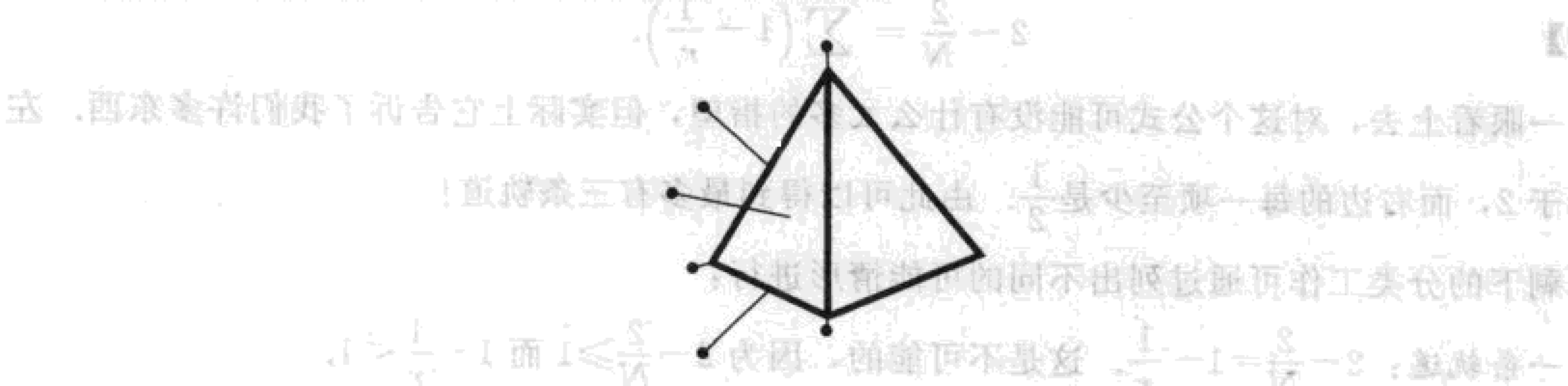






185

我们将不试图对无限子群进行分类．

证明　设 G 是 SO_3 的有限子群，记其阶为 N．除了恒等映射外，G 的每个元素 g 是绕某条直线 ℓ 的旋转，而这条直线显然是唯一的．因而 g 恰好保持 $\mathbb{R}^3$ 中的单位球面 S 的两个点不动，即交 $\ell \cap S$ 的两个点．我们把这两个点称为 g 的极点．这样一个极点是单位球面上的点 p，对 G 的某个元素 $g \neq 1$ 满足 $gp=p$．例如，若 G 是四面体 Δ 的旋转对称群，则极点是 S 上位于 Δ 的顶点上面、面的中心上面或边的中点上面的点．

184



用 P 表示所有极点的集合．

【9.2】引理　*集合 P 被 G 在球面上的作用映到自身．因而 G 在 P 上作用．*

证明　设 p 是一个极点，比如它是 $g \in G$ 的极点．设 x 是 G 的任意元素．我们要证明 xp 是一个极点，也就是说证明 xp 在 G 的某个不是单位元的元素 g' 的作用下不变．所需的元素为 xgx^{-1}：$xgx^{-1}(xp)=xgp=xp$，而因为 $g \neq 1$，$xgx^{-1} \neq 1$．■

我们现在通过数极点的个数得到关于群的信息．因为除了单位元 1，G 的每个元素有两个极点，我们的第一个猜测是共有 $2N-2$ 个极点．这是不对的，因为同一个点 p 可以是多于一个群元素的极点．

极点 p 的稳定子是在 G 中的所有围绕直线 $\ell=(0, p)$ 的旋转的群．这个群是循环群，它由在 G 中转过最小角度 θ 的旋转生成[见定理(3.4a)的证明]．如果稳定子的阶为 r_p，则 $\theta=\frac{2\pi}{r_p}$．

我们知道 $r_p>1$，因为，由于 p 是极点，稳定子 G_p 含有非单位元的元素．由计数公式(7.2)，

$$|G_p||O_p|=|G|.$$

将这个等式写为

【9.3】

$$r_p n_p = N,$$

其中 n_p 是 p 的轨道 O_p 中极点的个数．

G 中具有给定极点 p 的元素的集合是稳定子 G_p，减去单位元．于是有 (r_p-1) 个以 p 为极点的群元素．另一方面，除了 1 之外的每个群元素有两个极点．处处都得减去 1 有点使人糊涂，正确的关系是

【9.4】

$$\sum_{p\in P}(r_p-1) = 2N-2.$$

如果 p 与 p' 属于同一轨道，则稳定子 G_p 和 $G_{p'}$ 有相同的阶．这是由于 $O_p=O_{p'}$ 且 $|G|=|G_p||O_p|=|G_{p'}||O_{p'}|$．因而可将(9.4)左边对应于一条给定轨道 O_p 中的极点的各项集中起来．有 n_p 个这样的项，因而集中起来的极点的个数是 $n_p(r_p-1)$．我们将轨道以某种方式编号，如 O_1，O_2，…．则

185

$$\sum_i n_i(r_i-1) = 2N-2,$$

其中 $n_i=|O_i|$，且 $r_i=|G_p|$ 对任一 $p\in O_i$ 成立．因为 $N=n_i r_i$，可在两边除以 N，并交换两边，就得到著名的公式

【9.5】

$$2-\frac{2}{N} = \sum_i\left(1-\frac{1}{r_i}\right).$$

一眼看上去，对这个公式可能没有什么太多的指望，但实际上它告诉了我们许多东西．左边小于 2，而右边的每一项至少是 $\frac{1}{2}$．由此可以得到最多有三条轨道！

剩下的分类工作可通过列出不同的可能情形进行：

一条轨道：$2-\frac{2}{N}=1-\frac{1}{r}$．这是不可能的，因为 $2-\frac{2}{N}\geqslant 1$ 而 $1-\frac{1}{r}<1$．

两条轨道：$2-\frac{2}{N}=\left(1-\frac{1}{r_1}\right)+\left(1-\frac{1}{r_2}\right)$，即 $\frac{2}{N}=\frac{1}{r_1}+\frac{1}{r_2}$．

我们知道 $r_i\leqslant N$，因为 r_i 整除 N．这个等式成立仅当 $r_1=r_2=N$．这样 $n_1=n_2=1$．有两个极点 p，p'，它们都被群的每一个元素固定保持不变．显然，G 是围绕过 p 和 p' 的直线 ℓ 的旋转的循环群 C_n．

三条轨道：这是主要情形：公式(9.5)化为

$$\frac{2}{N}=\frac{1}{r_1}+\frac{1}{r_2}+\frac{1}{r_3}-1.$$

将 r_i 按增序排列．则 $r_1=2$．因为如果所有的 r_i 都至少为 3，则右边将 $\leqslant 0$，这是不可能的．

情形 1：至少两个阶 r_i 是 2：$r_1=r_2=2$．第三个阶 $r_3=r$ 可任意，而 $N=2r$．则 $n_3=2$：存在一对极点 $\{p, p'\}$ 形成轨道 O_3．每个元素 g 或使 p 和 p' 不动或使之互换．因而 G 的元素要么是绕直线 $\ell=(p, p')$ 的旋转，要么是绕与 ℓ 垂直的直线 ℓ' 转过 π 的旋转．容易看出 G 是使一个正 r-边形 Δ 不动的旋转群，即二面体群 D_r．多边形 Δ 位于与 ℓ 垂直的平面上，Δ 的顶点和面的中心对应剩下的极点．当把 Δ 放到 $\mathbb{R}^3$ 中时，$\mathbb{R}^2$ 中多边形的双侧(反射)对称成为了转过角度 π 的旋转．

186

情形 2：只有一个 r_i 为 2：三元组 $r_1=2$，$r_2\geqslant 4$，$r_3\geqslant 4$ 是不可能的，因为 $\frac{1}{2}+\frac{1}{4}+\frac{1}{4}-1=0$．类似地，$r_1=2$，$r_2=3$，$r_3\geqslant 6$ 也不会发生，这是因为 $\frac{1}{2}+\frac{1}{3}+\frac{1}{6}-1=0$．剩下的只有三种可能：

【9.6】

(i) $r_i=(2, 3, 3)$，$N=12$；

(ii) $r_i=(2, 3, 4)$，$N=24$；

(iii) $r_i=(2, 3, 5)$，$N=60$．

下面就分析这三种情形．我们简要地说明其形状．

【9.7】

(i) $n_i=(6, 4, 4)$．轨道 O_2 中的极点是一个正四面体 Δ 的顶点，且 G 是使之不变的旋转的群：$G=T$．这里 n_1 是 Δ 的边的条数，而 n_2，n_3 是 Δ 的顶点和面的数目．

(ii) $n_i=(12, 8, 6)$．O_2 中的极点是一个立方体的顶点，O_3 中的极点是一个正八面体的顶点．$G=O$ 是它们的旋转的群．整数 n_i 是立方体的边、顶点和面的个数．

(iii) $n_i=(30, 20, 12)$：O_2 中的极点是一个正十二面体的顶点，O_3 中的极点是一个正二十面体的顶点：$G=I$．

要证(9.7)的断言还有一些事要做．直观上，一条轨道上的极点应该是正多面体的顶点，因为它们构成单独一条轨道，因而均匀地分布在球面上．然而这并不太精确，例如，像立方体边的中点构成唯一的轨道，但却不能张成一个正多面体．(它们张成的图形称为截多面体．)

作为例子，考虑(9.7iii)．设 p 是 O_3 的 12 个极点之一，设 q 是 O_2 的最靠近 p 的极点．因为 p 的稳定子的阶为 5 且在 O_2 上作用(因为 G 在其上作用)，q 的象给出了 p 的最近的五个邻点的集合，这些邻点为由 q 通过 G 中五个绕 p 的旋转得到的极点．因而 O_2 中最靠近 p 的极点的个数是 5 的倍数，容易看出，5 是仅有的可能性．因此这五个极点是正五边形的顶点．这样定义的 12 个五边形构成了正十二面体． ■

在本章结束时，我们指出对于平面运动的讨论在 3-空间的刚体运动群 M_3 有类似结果．特别是可以定义晶体群，这是平移群是三维格 L 的离散子群．说 L 是格是指存在 $\mathbb{R}^3$ 中三个线性无关的向量 a，b，c 使得 t_a，t_b，$t_c\in G$．结晶群与 $M=M_2$ 中的格群类似，三维结构中的晶体形状以这样的群为其对称结构的例子．我们想象晶体无限大．则分子规则排列这一事实蕴涵它们形成一个具有三个无关平移对称的阵列．与存在 17 个格群类似，可以证明存在 230 类结晶群．这些群的列表太长而不太有用，因而晶体被粗分为七个晶体系．对于这方面更多的内容以

187

及对于 32 个晶体点群的讨论，请参看有关晶体的书.

一个好的传统比最有趣的几何问题更有价值，

因为它保持了一般方法并且有助于很好地解决问题.

Gottfried Wilhelm Leibnitz

练　习

第一节　平面图形的对称

1. 证明平面上一个图形 F 的对称的集合构成一个群.
2. 列出(a)正方形和(b)正五边形的所有对称.
3. 列出下列图形的所有对称.

   (a)(1.4)　(b)(1.5)　(c)(1.6)　(d)(1.7)
4. 设 G 是平面上绕原点旋转的有限群. 证明 G 是循环群.

第二节　平面运动群

1. 用代数方法计算 $t_a\rho_\theta$ 的不动点.
2. 利用定义(2.3)，通过直接计算验证规则(2.5).
3. 证明 $\boldsymbol{O}$ 不是 $\boldsymbol{M}$ 的正规子群.
4. 设 m 是一个反向运动. 证明 m^2 是平移.
5. 用 SM 表示平面上保向运动的子集. 证明 SM 是 M 的正规子群，并确定它在 M 中的指标.
6. 证明$\mathbb{R}^2$ 的线性算子是反射当且仅当其特征值为 1 和 −1，且其特征向量正交.
7. 证明反射或滑动反射的共轭是同类型的运动，且如果 m 是滑动反射，则 m 的滑动向量与其共轭的滑动向量有相同的长度.
8. 完成(2.13)是同态的证明.
9. 证明由 $t_a\rho_\theta \rightsquigarrow 1$ 与 $t_a\rho_\theta r \rightsquigarrow r$ 定义的映射 $M \longrightarrow \{1, r\}$是同态.

188

10. 计算在一个运动的表达式 $t_a\rho_\theta$ 和 $t_a\rho_\theta r$ 上，当其轴转过一个角度 η 的旋转的效果.
11. (a) 计算线性算子 $m=\rho_\theta r$ 的特征值和特征向量.

    (b) 用代数方法证明 m 是一个关于过原点的一条与 x-轴的夹角为$\frac{1}{2}\theta$ 的直线的反射.

    (c) 用几何方法证明(b)的结论.
12. 用 a 和 θ 计算出滑动 $t_a\rho_\theta r$ 的滑动向量.
13. (a) 设 m 是沿直线 ℓ 的滑动反射. 用几何方法证明点 x 在 ℓ 上当且仅当 x，$m(x)$，$m^2(x)$共线.

    (b) 反之，证明若 m 是保向运动，且 x 是一个点，满足 x，$m(x)$，$m^2(x)$是在一条直线 ℓ 上的不同的点，则 m 是沿直线 ℓ 的滑动反射.
14. 求由群 SM 到形如$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$(其中 $|a|=1$)的矩阵的 $GL_2(\mathbb{C})$的子群的同构.
15. (a) 用复变量 $z=x+\mathrm{i}y$ 的形式写出运动(2.3)的公式.

    (b) 证明每个运动具有 $m(z)=\alpha z+\beta$ 或 $m(z)=\alpha \bar{z}+\beta$ 的形式，其中 $|\alpha|=1$ 而 β 是任意复数.

第三节　有限运动群

1. 设 D_n 表示二面体群(3.6). 在 D_n 中把积 $x^2yx^{-1}y^{-1}x^3y^3$ 表成 x^iy^j 的形式.

2. 列出群 D_4 的所有子群，并确定哪些是正规的.
3. 求出群 D_{13} 和 D_{15} 的所有正规子群并确定其商群.
4. (a) 具体计算出二面体群 D_{10} 的子群 $H=\{1, x^5\}$ 的陪集.
   (b) 证明 D_{10}/H 同构于 D_5.
   (c) D_{10} 是否同构于 $D_5\times H$?
5. 列出 $G=D_6$ 中不包含子群 $N=\{1, x^3\}$ 的子群.
6. 证明 M 的每一个有限子群都是推论(3.5)中列出的标准子群之一的共轭子群.

第四节 离散运动群

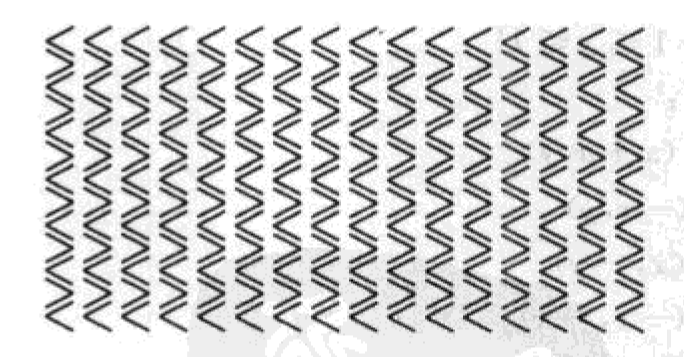
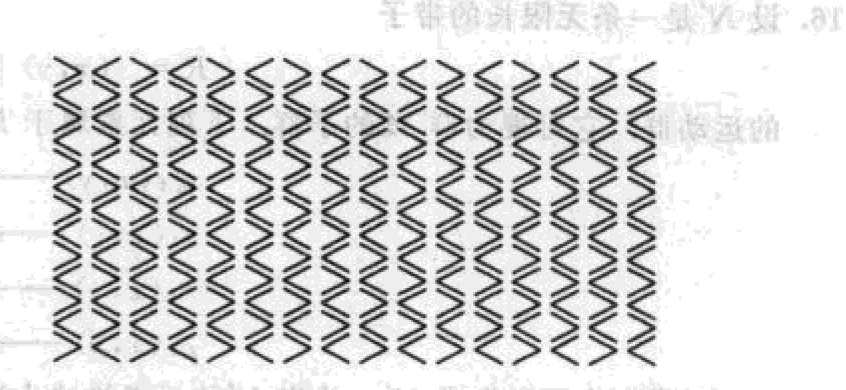
1. 证明绕原点的旋转组成的离散群 G 是循环群，并且是由 ρ_θ 生成，其中 θ 是 G 中旋转所转过的最小角度.
2. 设 G 是 M 的子群，它包含绕两个不同的点的旋转. 用代数方法证明 G 包含一个平移.
3. 设(a, b)是$\mathbb{R}^2$ 中一个格 L 的格基. 证明其他任意格基具有$(a', b')=(a, b)P$ 的形式，其中 P 是一个行列式为±1 的2×2 整数矩阵.
4. 确定图(4.16)中描绘的图案中每一个的点群.
5. (a) 设 B 是边长为a 的正方形，并设 $\epsilon>0$. 设 S 是 B 中的子集，满足 S 中任意两点间的距离$\geqslant\epsilon$. 求 S 中元素个数的准确上界.
   (b) 对$\mathbb{R}^n$ 中的方盒 B 做同样的事.

189

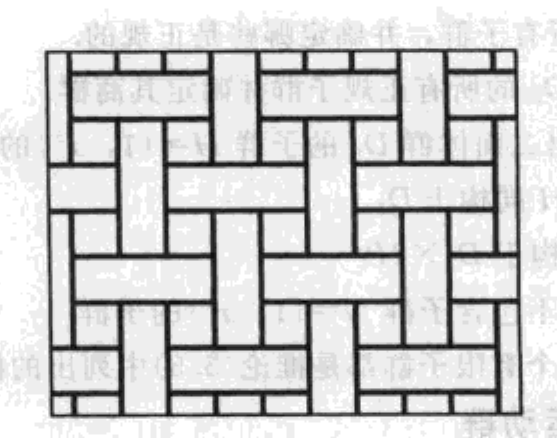
6. 证明$\mathbb{R}^+$ 中由 1 和$\sqrt{2}$生成的子群在$\mathbb{R}^+$ 中稠密.
7. 证明 $\boldsymbol{O}$ 的每一个离散子群是有限的.
8. 设 G 是 M 的离散子群. 证明存在平面上一点 p_0，它不是由 R 中除了单位元以外任意点的不动点.
9. 证明装饰图案

$$\ldots \text{ЄЄЄЄЄЄЄЄЄЄЄ} \ldots$$

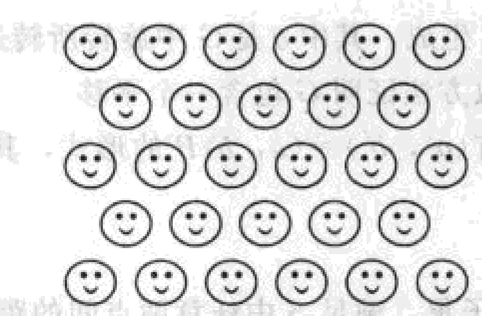
   的对称群同构于二阶循环群和无限循环群的直积 $C_2\times C_\infty$.
10. 设 G 是装饰图案 …ᒣᒧᒣᒧᒣᒧᒣᒧ… 的对称群.
   (a) 确定 G 的点群 $\overline{G}$.
   (b) 对每个元素$\overline{g}\in\overline{G}$ 和每个代表$\overline{g}$ 的元素 $g\in G$，几何地描述 g 的作用.
   (c) 设 H 是 G 的平移子群. 确定$[G:H]$.
11. 设 G 是图案

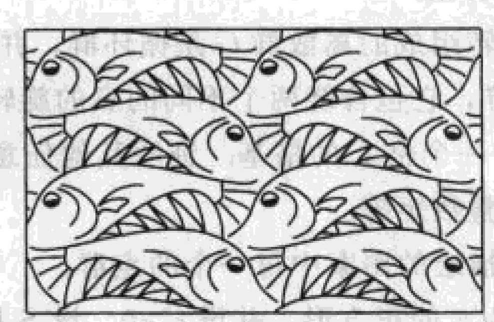



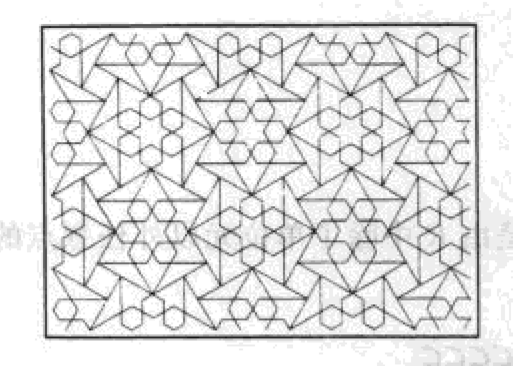
   的对称群. 确定 G 的点群.
12. 设 G 是一个等边三角格 L 的对称群. 求子群 $T\cap G$ 在 G 中的指标.
13. 设 G 是每个元素都保向的离散群. 证明点群 $\overline{G}$ 是旋转的循环群，且存在平面上的点 p 使得使 p 不动的群元素的集合同构于$\overline{G}$.
14. 对下面所示的图案，找出(4.16)中具有相同对称类型的图案.

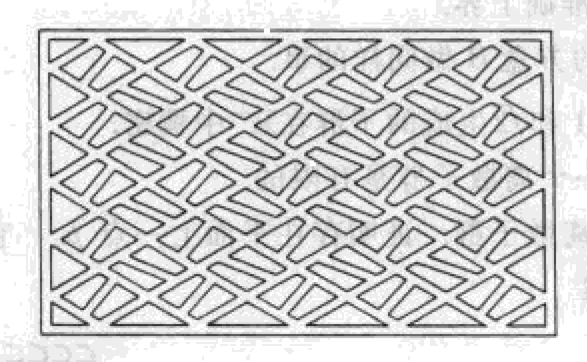


190









15. 用 N 表示直线 $\ell=\mathbb{R}^1$ 的刚体运动群. N 的一些元素为

$$t_a: x \longrightarrow x+a,\quad a\in\mathbb{R},\quad s: x \longrightarrow -x.$$

(a) 证明$\{t_a,\ t_a s\}$是 N 的所有元素，并几何地描述它们在 ℓ 上的作用.

(b) 计算积 $t_a t_b$，st_a，ss.

(c) 求 N 的包含一个平移的所有离散子群. 针对特别的子群来选择原点和单位长度会很方便. 证明你所列出的子群是完全的.

*16. 设 N'是一条无限长的带子

$$R=\{(x,y)\mid -1\leqslant y\leqslant 1\}$$

的运动群. 它可视为群 M 的子群. 下列元素属于 N'：

$$t_a:(x,y)\longrightarrow(x+a,y)$$
$$s:(x,y)\longrightarrow(-x,y)$$
$$r:(x,y)\longrightarrow(x,-y)$$
$$\rho:(x,y)\longrightarrow(-x,-y).$$

(a) 证明这些元素生成 N'，并将 N'的元素描述为这些元素的积.

(b) 对这些运动叙述并证明(2.5)的类似结果.

(c)在其对称群离散的意义下，装饰图案为带子上周期而非退化的任意图案. 因为它是周期的，其对称群将包含一个平移. 在(1.3)、(1.4)、(1.6)、(1.7)中显示了一些样板图案. 对出现的对称群进行分类，将那些仅在带子上原点和单位长度的选择上有差别的群等同起来. 建议先试着做具有不同种类的对称的图案. 当证明你的结论时请作细致的情形分析. 适当的形式如下：设 G 是包含一个平移的离散群.

191

情形 1：每个 G 的元素都是平移．则….

情形 2：G 包含旋转但不含反向对称．则，…，等等．

*17. 设 L 是 $\mathbb{R}^2$ 的格，并设 a，b 是 L 中线性无关的向量．证明 L 中由 a，b 生成的子群 $L'=\{ma+nb \mid m, n\in\mathbb{Z}\}$ 的指标是有限的，且其指标是在顶点为 0，a，b，$a+b$ 的平行四边形中且不在"远边"$[a, a+b]$和$[b, a+b]$上的格点的个数．（这样，包括 0，也包括了除 a，b 自己外的边$[0, a]$，$[0, b]$上的点．）

18. (a) 求平面上不被任何运动 $m\in M$ 固定的点的子集 F.

(b) 设 G 是离散运动群．证明 F 在 G 的元素下的所有象的并 S 是其对称群 G' 包含 G 的一个子集.

(c) 举例说明 G' 可以比 G 大.

*(d) 证明存在子集 F 使得 $G'=G$.

*19. 设 G 是格群，满足没有元素 $g\neq 1$ 使平面上的任一点不动．证明 G 由两个平移生成，或由一个平移和一个滑动生成.

*20. 设 G 是其点群是 $D_1=\{1, r\}$ 的格群.

(a) 证明 G 的所有滑动线和反射线都平行.

(b) 设 $L=L_G$．证明 L 包含非零向量 $a=(a_1, 0)^t$，$b=(0, b_2)^t$.

(c) 设 a 和 b 表示(b)中所示类型的最小向量．则(a, b)或(a, c)是 L 的一个格基，其中 $c=\frac{1}{2}(a+b)$.

(d) 证明如果选择平面坐标系使得 x-轴为滑动线，则 G 包含两个元素 $g=r$ 和 $g=t_{\frac{1}{2}a}r$ 之一．在这两种情形皆有$G=L\cup Lg$.

(e) 在(d)和(c)的描述中有四种可能性．证明只有三种不同类型的群.

21. 证明如果一个格群 G 的点群是 C_6，则 $L=L_G$ 是一个等边三角格，且 G 是 L 围绕原点的所有旋转对称的群.

22. 证明如果一个格群 G 的点群是 D_6，则 $L=L_G$ 是一个等边三角格，且 G 是 L 的所有对称的群.

*23. 证明图(4.16)所示的图形的对称群给出了所有的可能情形.

第五节　抽象对称：群作用

1. 求下列群的自同构群.

(a) C_4　(b) C_6　(c) $C_2\times C_2$

2. 证明(5.4)是一个等价关系.

3. 设 S 是集合，G 在其上作用．证明如果 $s'=gs$ 对某个 $g\in G$ 成立，则关系 $s\sim s'$是一个等价关系.

4. 设 $\varphi: G\longrightarrow G'$是一个同态，$S$ 是集合且 G'在其上作用．指出如何利用同态 φ 定义一个 G 在 S 上的作用.

5. 设 $G=D_4$ 是正方形对称的二面体群.

(a) 顶点的稳定子是什么？边的呢？

(b) G 在由对角线组成的二元集合上作用．对角线的稳定子是什么？

6. 在第四节练习 14 的每个图形上，求有非平凡稳定子的点，确定其稳定子.

*7. 设 G 是 M 的离散子群.

(a) 证明点 p 的稳定子 G_p 有限.

(b) 证明点 p 的轨道 O_p 是离散集，即存在一个数 $\varepsilon>0$ 使得轨道中任意两个点之间的距离至少是 ε.

(c) 设 B，B'是平面上两个有界区域．证明只存在有限多个 $g\in G$ 使得 $gB\cap B'$非空.

8. 设 $G=GL_n(\mathbb{R})$在集合 $S=\mathbb{R}^n$ 上以左乘作用.

(a) 描述 S 在这个作用下的轨道分解.

192

(b) e_1 的稳定子是什么？

9. 对于 $GL_2(\mathbb{C})$ 的下列作用，分解 2×2 复矩阵集合 $\mathbb{C}^{2\times 2}$.

(a) 左乘

(b) 共轭

10. (a) 设 $S=\mathbb{R}^{m\times n}$ 是实 $m\times n$ 矩阵的集合，并设 $G=GL_m(\mathbb{R})\times GL_n(\mathbb{R})$. 证明规则 $(P, Q), A \rightsquigarrow PAQ^{-1}$ 定义了 G 在 S 上的作用.

(b) 刻画 S 的 G-轨道分解.

(c) 设 $m\leqslant n$. 矩阵 $[I\mid 0]$ 的稳定子是什么？

11. (a) 刻画矩阵 $\begin{bmatrix}1 & 0\\0 & 2\end{bmatrix}$ 在 $GL_2(\mathbb{R})$ 共轭作用之下的轨道和稳定子.

(b) 考虑 $GL_2(\mathbb{F}_3)$ 中的矩阵，求轨道的阶(元素的个数).

12. (a) 定义域的自同构.

(b) 证明有理数域 $\mathbb{Q}$ 除了恒等映射以外没有别的自同构.

(c) 当 $F=\mathbb{Q}[\sqrt{2}]$ 时，求 Aut$F$.

第六节 对陪集的作用

1. 对于 G 在 G/H 上的作用，陪集 aH 的稳定子是什么？

2. 设 G 是群，并设 H 是由 G 的元素 x 生成的循环子群. 证明如果用 x 左乘使 G 中 H 的每个左陪集不动，则 H 是正规子群.

3. (a) 当 G 是二面体群 D_4 而 S 是正方形顶点的集合时，具体写出双射(6.4).

(b) 对 D_n 和正 n 边形的顶点作同样的事.

4. (a) 对于对称群 $G=S_n$ 在 $\{1, \cdots, n\}$ 上的作用具体刻画指标 1 的稳定子 H.

(b) 对这个作用具体刻画 G 中 H 的陪集.

(c) 具体刻画映射(6.4).

193

5. 刻画 S_3 在四个元素集合上的所有作用方式.

6. 证明命题(6.5).

7. G-集合的映射 $S \longrightarrow S'$ 称为 G-集合的同态，如果对所有 $g\in G$ 和 $s\in S$ 有 $\varphi(gs)=g\varphi(s)$. 设 φ 是一个这样的同态. 证明下面的结论：

(a) 稳定子 $G_{\varphi(s)}$ 包含稳定子 G_s.

(b) 元素 $s\in S$ 的轨道映到 $\varphi(s)$ 的轨道上.

第七节 计数公式

1. 利用计数公式确定立方体的旋转对称群的阶和正四面体的旋转对称群的阶.

2. 设 G 是立方体 C 的旋转对称群. 两个正四面体 Δ，Δ' 可以内接在 C 中，每个用其一半顶点. Δ 的稳定子的阶是什么？

3. 当允许像平面反射这样的反向对称和旋转时，计算正十二面体对称群的阶. 对立方体和正四面体做同样的计算.

4. 设 G 是立方体的旋转对称群，设 S_v，S_e，S_f 是立方体顶点、边和面的集合，并设 H_v，H_e，H_f 为顶点、边和面的稳定子. 求代表三个集合中的每一个对于其每一个子群的分解为轨道的公式.

5. 设 $G\supset H\supset K$ 是群. 不假设 G 有限，证明公式 $[G:K]=[G:H][H:K]$.

6. (a) 证明如果 H 和 K 是 G 的指标有限的子群，则交 $H\cap K$ 的指标也有限.

(b) 举例说明指标 $[H:H\cap K]$ 不必整除 $[G:K]$.

第八节　置换表示

1. 确定正四面体群 T(见(9.1))在二元集上的所有作用方式.
2. 设 S 是集合，群 G 在其上作用，且设 $H=\{g\in G \mid$ 对所有 $s\in S$，$gs=s\}$. 证明 H 是 G 的正规子群.
3. 设 G 是正方形对称的二面体群. G 在顶点上的作用是忠实的吗？在对角线上的作用呢？
4. 设群 G 在集合 S 上的作用有两条轨道，它们的阶分别为 m 和 n. 利用这个作用定义 G 到对称群的积 $S_m\times S_n$ 的同态.
5. 一个群 G 在五个元素的集合 S 上忠实地作用，它有两条轨道，一条的阶为 3 而另一条的阶为 2. G 可能是什么呢？
6. 完成命题(8.2)的证明.
7. 设 $F=\mathbb{F}_3$. 列向量空间 F^2 有四个一维子空间. 刻画这些子空间. 用可逆距阵左乘可置换这些子空间. 证明这个作用定义一个同态 $\varphi:GL_2(F)\longrightarrow S_4$. 确定这个同态的核和象.

194

*8. 对下面每个群求最小整数 n，使得群在 n 元集上有忠实作用.

  (a) 四元数群 H　(b) D_4　(c) D_6

第九节　旋转群的有限子群

1. 刻画正八面体和正二十面体旋转群的极点的轨道.
2. 确定垒球的对称群，考虑到缝合并允许反向对称.
3. 设 O 是立方体的旋转群. 求连接对顶的对角线的稳定子.
4. 设 $G=O$ 是立方体的旋转群，并设 H 是将其两个内接正四面体之一映到自己的子群(见第七节练习 2). 证明 $H=T$.
5. 证明正二十面体群有 10 阶子群.
6. 求下列群的所有子群：

  (a) T　(b) I

7. 解释为什么对于立方体及正八面体和对于正十二面体及正二十面体，其对称群是相等的.

*8. (a) 如果适当选择 α，则 12 个点$(\pm1,\pm\alpha,0)$，$(0,\pm1,\pm\alpha)$，$(\pm\alpha,0,\pm1)$构成正二十面体的顶点. 验证这一点，并确定 α.

  (b) 确定围绕$\mathbb{R}^2$ 的原点转过角度$\frac{2\pi}{5}$的旋转的矩阵.

  (c) 确定$\mathbb{R}^3$ 中围绕含有点$(1,\alpha,0)$的轴转过角度$\frac{2\pi}{5}$的旋转的矩阵.

*9. 证明三维晶体群的晶体限制：晶体的旋转对称的阶为 2，3，4 或 6.

杂题

1. 刻画下列群：

  (a) $\mathrm{Aut}D_4$.　(b) $\mathrm{Aut}H$，其中 H 是四元数群.

2. (a) 证明群 G 的自同构的集合 $\mathrm{Aut}G$ 构成一个群.

  (b) 证明由 $g\rightsquigarrow$(由 g 定义的共轭)定义的映射 $\varphi:G\longrightarrow \mathrm{Aut}G$ 是一个同态并确定其核.

  (c) 由群的元素的共轭形成的自同构称为内自同构. 证明内自同构的集合，也就是 φ 的象，是 $\mathrm{Aut}G$ 的正规子群.

3. 对四元数群 H，确定商群 $\mathrm{Aut}H/\mathrm{Int}H$.

*4. 设 G 是格群. G 的一个基本域 D 是平面上的一个有界区域，它由分段光滑曲线界定，使得集合 $gD(g\in G)$ 覆盖了平面，并且除了边界以外没有重叠. 我们假设 D 仅有有限多个连通分支.

  (a) 求第四节练习 14 所示图案的对称群的基本域.

  (b) 证明 G 的两个基本域 D，D'可以分割为有限多个形如 $gD\cap D'$或 $D\cap gD'$的全等块(见第五节练习 7).

195

(c) 推断 D 和 D' 有相同的面积.（可能出现边界曲线无限次相交，这引出关于面积定义的问题. 在你的回答中忽略这一点.）

*5. 设 G 是格群，并设 p_0 是平面上的点，它不被 G 的任意元素保持不变. 设 $S=\{gp_0 \mid g\in G\}$ 是 p_0 的轨道. 平面可如下分成多边形，使每个多边形中只含有一个 S 的点：含有点 p 的多边形 Δ_p 是距 p 点距离为到 S 中任意点的距离的最小距离的点集：

$$\Delta_p = \{q \in \mathbb{R}^2 \mid \mathrm{dist}(q,p) \leqslant \mathrm{dist}(q,p') \text{ 对所有 } p' \in S \text{ 成立}\}.$$

(a) 证明 Δ_p 是多边形.

(b) 证明 Δ_p 是 G 的基本域.

(c) 证明本方法除了构造的域 Δ_p 不必是有界集的情形外，对所有 M 的离散子群都适用.

(d) 证明 Δ_p 是有界集当且仅当 G 是格群.

*6. (a) 设 $G'\subset G$ 是两个格群. 设 D 是 G 的基本域. 证明 G' 的基本域 D' 可由 D 的有限多个平移 gD 构造.

(b) 证明 $[G:G']<\infty$，并且 $[G:G']=\dfrac{\text{面积}(D')}{\text{面积}(D)}$.

(c) 对图案(4.16)中的每一个计算指标 $[G:L_G]$.

*7. 设 G 是在有限集合 S 上作用的有限群. 对每个元素 $g\in G$，用 S^g 表示在 g 下不变的 S 的元素的子集：$S^g=\{s\in S \mid gs=s\}$.

(a) 我们可以想象断言 $gs=s$ 的真值表，比如行以 G 中元素为指标而列以 S 中元素为指标. 对二面体群 D_3 在一个三角形的顶点上的作用构造这样的表.

(b) 证明公式 $\sum\limits_{s\in S} |G_s| = \sum\limits_{g\in G} |S^g|$.

(c) 证明伯恩赛德公式：

$$G\cdot(\text{轨道个数}) = \sum_{g\in G} |S^g|.$$

8. 存在 $70=\binom{8}{4}$ 种对八边形的边着色的方法，使之有四条黑边四条白边. 群 D_8 在这个 70 个元素的集合上作用，轨道代表等价的着色. 用伯恩赛德公式计算等价类的个数.

9. 设 G 是 n 阶群，它在一个 r 阶集合上非平凡地作用. 证明若 $n>r!$，则 G 有真的正规子群.

第六章　群论的进一步讨论

要做或要证明的越多，做起来或证明起来就越容易

James Joseph Sylvester

第一节　群在自身的作用

我们说群 G 在自身上的作用，是指在作用的定义中，G 同时扮演群和它所作用的集合的角色．每个群都以各种方式对其自身作用，这里我们选出其中两个．第一个是左乘：

【1.1】
$$G\times G\longrightarrow G$$
$$g,x \rightsquigarrow gx.$$

这显然是 G 在 G 上的一个可迁作用，即 G 构成单独一条轨道，并且任意元素的稳定子都是单位元子群 $\{1\}$．因而作用是忠实的，并且第五章第八节定义的同态

【1.2】
$$G\longrightarrow \mathrm{Perm}(G)$$
$$g \rightsquigarrow m_g = \text{用 } g \text{ 左乘}$$

是单射．

【1.3】定理　*凯莱定理：每一个有限群同构于某个置换群的子群．如果 G 的阶为 n，则它同构于对称群 S_n 的子群．*

证明　因为左乘作用是忠实的，G 同构于它在 $\mathrm{Perm}(G)$ 中的象．如果 G 的阶为 n，则 $\mathrm{Perm}(G)$ 同构于 S_n．■

197

虽然凯莱定理本身是很有意思的，但它对于计算并不特别有用，因为 S_n 具有阶 $n!$，它与 n 相比太大了．

我们要考虑的第二个作用更为微妙．这就是共轭，也就是由

【1.4】
$$(g,x)\rightsquigarrow gxg^{-1}$$

定义的映射 $G\times G\longrightarrow G$．由于显而易见的原因，我们将不用乘法记号表示这个作用．读者应该验证第五章的公理(5.1)，暂时用一个如 $g*x$ 的记号来表示共轭 gxg^{-1}．

元素 $x\in G$ 对于共轭作用的稳定子有一个特殊的名字．它称为 x 的**中心化子**，并记为 $Z(x)$：

【1.5】
$$Z(x)=\{g\in G\mid gxg^{-1}=x\}=\{g\in G\mid gx=xg\}.$$

中心化子是 G 中与 x 可置换的群元素的集合．注意 $x\in Z(x)$，因为 x 与自己可置换．

对于共轭作用，x 的轨道称为 x 的**共轭类**．它由所有共轭元素 gxg^{-1} 组成．我们常将共轭类写作

【1.6】
$$C_x=\{x'\in G\mid \text{对某个 } g\in G \text{ 有 } x'=gxg^{-1}\}.$$

由计数公式[第五章(7.2)]，$|G|=|C_x|\,|Z(x)|$．

因为共轭类是群作用的轨道，它们划分了群 G．这给出了我们称之为有限群的**类方程**的公式[见第五章(7.3)]：

【1.7】 $$|G| = \sum_{\text{共轭类}C} |C|.$$

如果对共轭类编号，比如记为 C_i，$i=1$，…，k，则这个公式成为

$$|G| = |C_1| + \cdots + |C_k|.$$

然而这里容易引起混乱，因为 C_i 的下标 i 是一个指标，而在前面使用的记号中 C_x 代表包含 G 的元素 x 的共轭类．特别地，C_1 有两种含义．也许最好先将 G 的单位元素 1 的共轭类列出来．则 C_1 的两种解释将是一致的．

注意单位元被所有 $g \in G$ 保持不变．这样 C_1 只由元素 1 单独组成．还要注意(1.7)右边的每一项，作为轨道的阶，它们整除左边．这对于可能出现在这样的等式中的整数组合是一个很强的限制．

【1.8】*类方程右边的数整除群的阶，且其中至少有一个为 1.*

例如，二面体群 D_3 的共轭类按第五章(3.6)那样表出时，为下面三个子集：

198

$$\{1\}, \{x, x^2\}, \{y, xy, x^2 y\}.$$

两个旋转 x，x^2 是共轭的，三个反射也一样．D_3 的类方程是

【1.9】 $$6 = 1 + 2 + 3.$$

回忆第二章(4.10)，一个群 G 的中心是与群的所有元素可置换的元素的集合 Z：

$$Z = \{g \in G \mid 对所有\ x \in G, gx = xg\}.$$

一个元素 x 的共轭类由这个元素单独组成当且仅当对所有 $g \in G$ 有 $x = gxg^{-1}$．这表明 x 属于中心．这样中心的元素由类方程右边的 1 代表．

由定义直接得到下面的命题．

【1.10】命题 *一个元素 x 属于群 G 的中心当且仅当其中心化子 $Z(x)$ 是整个群.*

类方程(1.7)可以被有效应用的一种情形是当群 G 的阶是一个素数 p 的正幂．这样的群称为 p-群．下面是类方程在 p-群上的几个应用．

【1.11】命题 *p-群 G 的中心的阶 >1.*

证明 (1.7)的左边是 p 的幂，设为 p^e．右边的每一项也是 p 的幂，因为它整除 p^e．我们要证明某个群元素 $x \neq 1$ 属于中心，这和说(1.7)右边多于一项等于 1 是一样的．现在不是 1 的项都是 p 的正幂，可被 p 整除．假设类 C_1 是对右边唯一给出 1 的项．则等式成为

$$p^e = 1 + \sum (p\ 的倍数),$$

除非 $e=0$，否则这是不可能的． ■

可以把这个证明的过程反过来并加以抽象，从而给出下面这个重要的 p-群作用的不动点定理：

【1.12】命题 *设 G 是一个 p-群，并设 S 是一个有限集合，G 在它上面作用．假设 S 的阶不被 p 整除．则 G 在 S 上的作用有个不动点，即稳定子为整个群的元素 $s \in S$.*

【1.13】命题 *每个 p^2 阶的群是阿贝尔群.*

证明 设 G 是阶为 p^2 的群．我们证明对每一 $x \in G$，中心化子 $Z(x)$ 是整个群．这样命题(1.10)将完成证明．为此设 $x \in G$．若 x 在中心 Z 中，则如断言所述 $Z(x)=G$．若 $x \notin Z$，则 $Z(x)$ 严格大于 Z，因为它包含 Z 同时也包含元素 x．既然 Z 和 $Z(x)$ 的阶整除 $|G| = p^2$，而命题(1.11)告诉我

199

们 $|Z|$ 至少是 p．仅有的可能是 $|Z(x)| = p^2$．因而 $Z(x)=G$，最终 x 还是属于中心． ■

存在 p^3 阶的非阿贝尔群．例如二面体群 D_4 的阶为 8．

我们用(1.13)对 p^2 阶群进行分类．

【1.14】推论　每一 p^2 阶群是下列类型之一：

(i) p^2 阶循环群．

(ii) 两个 p 阶循环群的积．

证明　因为元素的阶整除 p^2，有两种情形需要考虑：

情形 1：G 包含 p^2 阶元素因而是循环群．

情形 2：G 中除单位元外每个元素 x 的阶为 p．设 x，y 是两个不等于 1 的元，并设 H_1，H_2 分别是由 x，y 生成的 p 阶循环群．我们可选择 y 使之不是 x 的幂．则由于 $y \notin H_1$，$H_1 \cap H_2$ 小于阶为 p 的 H_2．所以 $H_1 \cap H_2 = \{1\}$．又因为 G 是阿贝尔群，子群 H_i 都是正规的．因为 $y \notin H_1$，群 $H_1 H_2$ 严格大于 H_1，且其阶整除 p^2．这样 $H_1 H_2 = G$．由第二章(8.6)，$G \approx H_1 \times H_2$．■

p^n 阶可能的群的个数随 n 迅速增长．有 5 个 8 阶群的同构类，有 14 个 16 阶群的同构类．

第二节　二十面体群的类方程

本节我们确定十二面体的旋转对称的二十面体群 I 的共轭类，并用它们来研究这个非常有意思的群．正如我们已经看到的那样，二十面体群的阶是 60．它含有围绕十二面体的面的中心转过 $\frac{2\pi}{5}$ 的倍数的旋转、绕顶点转过 $\frac{2\pi}{3}$ 的倍数的旋转以及绕边的中心转过 π 的旋转．20 个顶点中的每一个都有一个 3 阶的稳定子，相对的顶点有相同的稳定子．这样共有 10 个阶为 3 的子群——顶点的稳定子．每个 3 阶子群含有两个 3 阶元素，且任意两个这样的子群的交只由单位元单独组成．因而 I 含有 $10 \times 2 = 20$ 个 3 阶元素．类似地，面有 5 阶稳定子，而且共有 6 个这样的稳定子，一共给出 $6 \times 4 = 24$ 个 5 阶元素．存在 15 个边的稳定子，这些稳定子的阶为 2．因而有 15 个 2 阶元素．最后，存在 1 个 1 阶元素．由于

【2.1】
$$60 = 1 + 15 + 20 + 24,$$

我们就列出了群的所有元素．

200

等式(2.1)由根据元素的阶对群划分得到．它与类方程有密切联系，但我们可以由(2.1)看到，它本身不是类方程，因为在右边出现的 24 不整除 60．另一方面，我们知道共轭的元素的确有相同的阶．这样类方程由对 G 的这一划分的进一步细分得到．还有，注意到 3 阶子群都共轭．这是群作用的一个一般性质，因为它们都是顶点的稳定子，而顶点构成单独一条轨道[第五章(6.5)]．同样的结果对 5 阶和 2 阶子群也成立．

显然，作为 2 阶共轭子群的非平凡元素，15 个 2 阶元素构成一个共轭类．3 阶元素怎么样呢？设 x 是围绕一个顶点 v 反时针转过 $\frac{2\pi}{3}$ 的旋转．虽然 x 将与绕任意其他顶点转过同样角度的旋转共轭[第五章(6.5)]，但 x 是否与 x^2 共轭并不清楚．第一个猜测也许应该是 x 与 x^2 不共轭．

用 v' 表示 v 对面的顶点，并设 x' 是围绕 v' 反时针转转过 $\frac{2\pi}{3}$ 的旋转．这样 x 和 x' 是群的共

轭元．注意围绕 v 的反时针旋转 x 与围绕其对面顶点 v' 顺时针旋转 $\frac{2\pi}{3}$ 是同一个运动．这样 $x^2=x'$，这说明 x 与 x^2 事实上是共轭的．由此得到所有 3 阶元素是共轭的．类似地，12 个转过 $\frac{2\pi}{5}$ 的旋转和转过 $-\frac{2\pi}{5}$ 的旋转是共轭的，它们同剩下的 12 个转过 $\frac{4\pi}{5}$，$-\frac{4\pi}{5}$ 的 5 阶旋转不共轭．（如我们已经注意到的，一个原因是共轭类的阶整除群的阶，而 24 不整除 60.）这样存在两个 5 阶元素的共轭类，并且类方程为

【2.2】
$$60 = 1+15+20+12+12.$$

我们将用这个类方程证明下面的定理．

【2.3】定理 *二十面体群 I 没有真的正规子群.*

群 $G\neq\{1\}$ 称为单群，如果它不是平凡群并且它不包含真的正规子群（除 $\{1\}$ 和 G 外没有别的正规子群）．这样定理可以复述为：

【2.4】 *二十面体群是单群.*

素数阶循环群根本不含真子群，因而是单群．所有其他群，除了平凡群外都含有真子群，虽然不必是正规的．我们应该强调这里的单字的使用并不意味着“不复杂”．它在这里粗略地意思为“不是合成的”．

201

定理(2.3)的证明 下面引理的证明是直接的．

【2.5】引理

(a) 如果 G 的正规子群 N 包含一个元素 x，则它包含 x 在 G 中的共轭类 C_x．换言之，正规子群是共轭类的并.

(b) G 的正规子群 N 的阶是它所包含的共轭类的阶的和.

我们现在应用这个引理．二十面体群的真正规子群的阶整除 60 且是类方程(2.2)右边的包括项 1 在内的一些项的和．碰巧不存在这样的整数．这就证明了定理． ■

【2.6】定理 *二十面体群与交错群 A_5 同构.*

证明 为描述这个同构，我们需要找到一个 I 在其上面作用的有五个元素的集合 S．一个这样的集合由内接于十二面体的五个立方体组成，其中一个的图示如下：

【2.7】图

十二面体的一个内接立方体

群 I 在这个立方体的集合 S 上作用，并且这个作用定义一个为相应的置换表示的同态 φ: $I \longrightarrow S_5$. 映射 φ 是由 I 到其象 A_5 的同构. 为证明它是一个同构，我们将用到 I 是一个单群这个事实，但需要很少的关于作用本身的信息.

由于 φ 的核是 I 的正规子群且由于 I 是单群，$\ker\varphi$ 或是 $\{1\}$ 或是 I. 说 $\ker\varphi = I$ 意味着 I 在五个立方体上的作用是平凡作用，但这是不对的. 因此 $\ker\varphi = \{1\}$，因而 φ 是单射，这定义了一个 I 到它在 S_5 中的象的一个同构.

我们把在 S_5 中的象也记作 I. 将符号同态 $S_5 \longrightarrow \{\pm 1\}$ 限制到 I，可得到一个同态 $I \longrightarrow \{\pm 1\}$. 如果这个同态是满射，其核将是 I 的一个 30 阶的正规子群[第二章(6.5)]. 由于 I 是单群，这是不可能的. 因而这个限制是个平凡同态，这恰好表明 I 包含在符号同态的核 A_5 之中. 因为两个群的阶都是 60，所以 $I = A_5$. ■

202

第三节 在子集上的作用

每当群 G 在集合 S 上作用时，也存在一个在子集上的作用. 若 $U \subset S$ 是一个子集，则

【3.1】
$$gU = \{gu \mid u \in U\}$$

是 S 的另一个子集. 作用公理的验证是显然的. 因此 G 在 S 的子集的集合上作用. 如果愿意的话，可以考虑在给定阶的子集上的作用. 因为用 g 乘是 S 的置换，所以子集 U 和 gU 有相同的阶.

例如，设 O 是立方体的 24 个旋转的八面体群，设 S 是立方体的顶点的集合. 考虑 O 在 S 的 2 阶子集上的作用，即在顶点的无序对上的作用. 共有 28 个这样的对，它们形成群的三条轨道：

(i) {边上的顶点对}；

(ii) {立方体一个面上的相对的顶点对}；

(iii) {立方体的相对的顶点对}.

这些轨道的阶分别是 12，12 和 4：$28 = 12 + 12 + 4$.

子集 U 的稳定子是使得 $gU = U$ 的群元素 g 的集合. 这样一个面上相对的顶点对的稳定子含有两个元素——恒等元和关于该面转过角度 π 的旋转. 这与计数公式相吻合：$24 = 2 \cdot 12$.

再次提请注意这一要点：等式 $gU = U$ 并不意味着 g 使 U 的元素不动，而是 g 置换 U 中的元素，即只要 $u \in U$ 就有 $gu \in U$.

【3.2】命题 *设 H 是在集合 S 上作用的群，且设 U 是 S 的子集. 则 H 稳定 U 当且仅当 U 是 H-轨道的并.*

该命题只不过是复述了元素 $u \in U$ 的 H-轨道是所有元素 hu 的集合. 若 H 稳定 U，则 U 包含其任意元的 H-轨道.

考虑 G 通过左乘在 G 的子集上的作用. G 的任意子群 H 都是子集，其轨道由左陪集组成. G 在陪集上的这个作用已在第五章(6.1)中定义. 但 G 的任意子集都有轨道.

【3.3】例 设 $G = D_3$ 是等边三角形的对称的二面体群，如通常方式表出：

$$G = \{x^i y^j \mid 0 \leqslant i \leqslant 2, 0 \leqslant j \leqslant 1, x^3 = 1, y^2 = 1, yx = x^2 y\}.$$

203

这个群含有 15 个 2 阶子集，我们可以将这个 15 元集分解成左乘的轨道. 有 3 个 2 阶子群：

【3.4】 $$H_1=\{1,y\},\quad H_2=\{1,xy\},\quad H_3=\{1,x^2y\}.$$

其陪集形成 3 个 3 阶轨道. 其他 6 个 2 阶子集构成单独一条轨道：15=3+3+3+6. 6 轨道是

【3.5】 $$\{1,x\},\{x,x^2\},\{x^2,1\},\{y,x^2y\},\{xy,y\},\{x^2y,xy\}.$$

【3.6】命题 *设 U 是群 G 的子集. 左乘作用下 U 的稳定子 Stab(U)的阶整除 U 的阶.*

证明 用 H 表示 U 的稳定子. 命题(3.2)告诉我们 U 是 H 在 G 上作用的一些轨道的并. 这些 H-轨道是右陪集 Hg. 因而 U 是右陪集的并. 从而 U 的阶是 $|H|$ 的倍数. ■

由于稳定子是 G 的子群，其阶当然也整除 $|G|$. 因而如果 $|U|$ 与 $|G|$ 无公因子，则 Stab(U)是平凡子群$\{1\}$.

共轭在 G 的子集上的作用也很有意思. 例如，可以将 D_3 的 15 个 2 阶子群划分为共轭的轨道. 共轭子群的集合$\{H_1, H_2, H_3\}$是一条轨道，集合$\{x, x^2\}$自己构成一条轨道. 其他轨道的阶为 2，3 和 6：15=1+2+3+3+6.

对于我们来说，重要的是一个子群 $H\subset G$ 在共轭作用下的轨道. 这个轨道是共轭子群的集合

$$\{gHg^{-1}\mid g\in G\}.$$

子群 H 是正规的当且仅当这个轨道由 H 独自组成，即对所有 $g\in G$，$gHg^{-1}=H$.

共轭作用下子群 H 的稳定子称为 H 的*正规化子*，记作

【3.7】 $$N(H)=\{g\in G\mid gHg^{-1}=H\}.$$

计数公式成为

【3.8】 $$|G|=|N(H)|\cdot|\{\text{共轭子群}\}|.$$

因此共轭子群的个数等于指标$[G:N(H)]$.

注意正规化子总是包含子群

【3.9】 $$N(H)\supset H,$$

这是因为当 $h\in H$ 时 $hHh^{-1}=H$. 于是由拉格朗日定理，$|H|$ 整除 $|N(H)|$，$|N(H)|$ 整除 $|G|$.

在例(3.3)中，子群 H_1，H_2，H_3 都是共轭的，因而 $|N(H_i)|=2$；于是 $N(H_i)=H_i$.

正规化子 $N(H)$的定义表明，H 是 $N(H)$的正规子群，事实上 $N(H)$是包含 H 为其正规子群的最大的群. 特别地，$N(H)=G$ 当且仅当 H 是 G 的正规子群.

第四节 西罗定理

我们本节将要证明的西罗定理描述了任意有限群的素数幂阶的子群.

设 G 是阶为 $n=|G|$ 的群，设 p 是一个整除 n 的素数. 我们将使用下面的记号：p^e 是 p 的整除 n 的最大的幂，这样

【4.1】 $$n=p^em$$

对整数 m 成立，而 p 不能整除 m.

【4.2】定理 *西罗第一定理：G 中存在一个阶为 p^e 的子群.*

西罗定理的证明放在本节最后.

【4.3】推论 *如果素数 p 整除有限群 G 的阶，则 G 中包含一个 p 阶元素.*

这是因为，设 H 是 p^e 阶子群，并设 x 是 H 中不等于 1 的元素. x 的阶整除 p^e，因而存在 $0<r\leqslant e$ 范围内的一个 r，使 x 的阶为 p^r. 于是 $x^{p^{r-1}}$ 的阶为 p.

没有西罗定理，这个推论并不是明显的. 我们已经知道任意元素的阶整除 $|G|$，但可以想象，比如说一个 6 阶群由单位元 1 和 5 个 2 阶元素组成. 这样的群是不存在的. 根据推论(4.3)，6 阶群必须含有一个 3 阶元素和一个 2 阶元素.

【4.4】推论 *恰好存在两个 6 阶群的同构类. 它们是循环群 C_6 和二面体群 D_3 的类.*

证明 设 x 是 G 中的 3 阶元素而 y 是 2 阶元素. 容易看出 6 个乘积 $x^iy^j(0\leqslant i\leqslant 2,\ 0\leqslant j\leqslant 1)$ 是群的不同元素. 因为可以将等式 $x^iy^j=x^ry^s$ 重新写成 $x^{i-r}=y^{s-j}$ 的形式. 对 x 的每个幂，除了单位元以外阶都为 3，而对 y 的每个幂，除了单位元以外阶都为 2. 这样 $x^{i-r}=y^{s-j}=1$，这表明 $r=i$ 和 $s=j$. 因为 G 的阶为 6，6 个元素 $1,x,x^2,y,xy,x^2y$ 构成整个群. 特别地，yx 必为其中之一. $yx=y$ 是不可能的，因为这将意味着 $x=1$. 类似地，$yx\neq 1,x,x^2$. 因而在 G 中

$$xy=yx \quad 或 \quad yx=x^2y$$

两个关系之一成立. 这两个关系之一，加上 $x^3=1$ 和 $y^2=1$，使我们能确定群的乘法表. 因而最多存在两个 6 阶群的同构类. 我们已经知道两个，即循环群 C_6 和二面体群 D_3 的类. 因此它们是仅有的 6 阶群. ■

205

【4.5】定义 *设 G 是一个 $n=p^em$ 阶群，其中 p 是不整除 m 的素数，且 $e\geqslant 1$. G 的 p^e 阶子群 H 称为 G 的西罗 p-子群，常把它称为西罗子群.*

这样西罗 p-子群是其指标不被 p 整除的 p-子群. 由定理(4.2)，如果 p 整除一个有限群 G 的阶，G 总有一个西罗 p-子群. 剩下的西罗定理(4.6)和(4.8)给出了关于它们的更多信息.

【4.6】定理 *西罗第二定理：设 K 是 G 的子群，其阶被 p 整除，设 H 是 G 的一个西罗 p-子群. 则存在一个共轭子群 $H'=gHg^{-1}$，使得 $K\cap H'$ 是 K 的一个西罗子群.*

【4.7】推论

(a) *设 K 是 G 的子群且是一个 p-群，则 K 包含在 G 的一个西罗 p-子群中.*

(b) *G 的所有西罗 p-子群都共轭.*

显然西罗子群的共轭也是西罗子群. 因而要得到推论的第一部分，只需注意一个 p-群 K 的西罗子群是群 K 自己. 因而如果 H 是西罗子群而 K 是一个 p-群，存在一个共轭 H' 使得 $K\cap H'=K$，也就是说 H' 包含 K. 对于(b)，设 K 和 H 是西罗子群. 则存在 H 的一个共轭 H' 包含 K. 因为它们的阶相等，所以 $K=H'$. 这样 K 与 H 共轭.

【4.8】定理 *西罗第三定理：设 $|G|=n$，而如(4.1)有 $n=p^em$. 设 s 是西罗 p-子群的个数. 则 s 整除 m 且同余于 1(模 p)：$s\mid m$，且对某个整数 $a\geqslant 0$，$s=ap+1$ 成立.*

在证明该定理之前，我们先用它们来确定 15 和 21 阶的群. 这些例子表明了西罗定理的威力有多大，但不要被误导. 当 n 有很多个因子时，n 阶群的分类是不容易的，可能性太多了.

【4.9】命题

(a) *每个 15 阶群都是循环群.*

(b) 存在两个 21 阶群的同构类：循环群 C_{21} 的类和有两个生成元 x，y 且满足关系 $x^7=1$，$y^3=1$，$yx=x^2y$ 的群 G 的类.

证明

(a) 设 G 是一个 15 阶群. 由(4.8)西罗 3-子群的个数整除 5 并且同余于 1(模 3). 这样的整数只有 1. 因而存在一个西罗 3-子群 H，并且由此它是一个正规子群. 由类似的推理，只有一个西罗 5-子群 K，并且它也是正规子群. 显然，$H\cap K=\{1\}$，因为 $K\cap H$ 的阶同时整除 5 和 3. 而且 KH 是阶 >5 的群，因而 $KH=G$. 由第二章(8.6)，G 同构于积群 $H\times K$. 这样任一 15 阶的群同构于阶为 3 和 5 的循环群的直积. 所有 15 阶的群都同构. 因为循环群 C_{15} 是它们中的一个，所以每个 15 阶群都是循环群.

(b) 设 G 是 21 阶群. 则定理(4.8)表明西罗 7-子群 K 必是正规的. 但是由定理不能排除存在 7 个共轭的西罗 3-子群 H 的可能性，事实上，这种情形确实会出现. 设 x 表示 K 的生成元，y 是西罗 3-子群之一 H 的生成元. 则 $x^7=1$，$y^3=1$，且由于 K 正规，对某个 $i<7$，$yxy^{-1}=x^i$ 成立.

我们可以用关系 $y^3=1$ 来限制指数 i 的可能取值. 这蕴涵

$$x=y^3xy^{-3}=y^2x^iy^{-2}=yx^{i^2}y^{-1}=x^{i^3}.$$

因此 $i^3\equiv 1(\bmod 7)$. 这表明 i 可以取值 1，2，4.

情形 1：$yxy^{-1}=x$. 群是阿贝尔群，且由第二章中的(8.6)，它同构于 3 阶和 7 阶循环群的直积. 这样的群是循环的[第二章(8.4)].

情形 2：$yxy^{-1}=x^2$. 在 G 中可以利用法则 $x^7=1$，$x^3=1$，$yx=x^2y$ 做乘法，将元素 x，y 的任意乘积简化为 x^iy^j 的形式，其中 $0\leqslant i<7$ 和 $0\leqslant j<3$. 我们将这个群的存在性的证明留作练习.

情形 3：$yxy^{-1}=x^4$. 在这种情形，我们用 y^2 代替 y，它也是 H 的一个生成元，从而化为前面的情形：$y^2xy^{-2}=yx^4y^{-1}=x^{16}=x^2$. 这样，正如我们所断言的，存在 21 阶群的两个同构类. ■

下面证明西罗定理.

西罗第一定理的证明 设 $\mathcal{S}$ 是 G 的所有 p^e 阶子集的集合. 这些子集中有一个是要求的，但我们不是直接求出它，而是证明这些子集中有一个具有 p^e 阶稳定子. 这个稳定子就是所求的子群.

【4.10】引理 在一个 $n=p^em$ 个元素(p 不整除 m)的集合中 p^e 阶子集的个数是二项式系数

$$N=\binom{n}{p^e}=\frac{n(n-1)\cdots(n-k)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots(p^e-k)\cdots 1}.$$

而且，N 不被 p 整除.

证明 p^e 阶子集的个数是这个二项式系数，这是一个标准的事实. 要证 N 不被 p 整除，注意每当 p 整除 N 的分子上的一项$(n-k)$时，它也整除分母上的项(p^e-k)恰好同样数量的次数：如果将 k 写为 $k=p^il$ 的形式，其中 p 不整除 l，则 $i<e$. 因而$(n-k)$和(p^e-k)都被 p^i 整除而不能被 p^{i+1} 整除. ■

我们将 $\mathcal{S}$ 分解为左乘作用的轨道，得到公式

$$N=|\mathcal{S}|=\sum_{\text{轨道}O}|O|.$$

因为 p 不整除 N，某个轨道有不为 p 所整除的阶，设它是子集 U 的轨道. 我们现在应用命题

(3.6)断定 $|\mathrm{Stab}(U)|$ 是 p 的幂. 因为由计数公式,

【4.11】 $$|\mathrm{Stab}(U)|\cdot|O_U|=|G|=p^e m,$$

而且因为 $|O_U|$ 不能被 p 整除, 由此得到 $|\mathrm{Stab}(U)|=p^e$. 这个稳定子就是所要求的子群. ■

西罗第二定理的证明 给定一个群 G 的子群 K 和一个西罗子群 H, 我们要证明对 H 的某个共轭子群 H', 交 $K\cap H'$ 是 K 的西罗子群.

用 S 表示左陪集 G/H 的集合. 对此集合我们需要的事实是 G 可迁地作用, 也就是说集合构成单独一条轨道, 且 H 是它的一个元素, 即 $s=1H$ 的稳定子. 因而 as 的稳定子是共轭子群 aHa^{-1}[见第五章(6.5b)].

我们将 G 的作用限制到 K 上, 并且将 S 分解为 K-轨道. 因为 H 是西罗子群, S 的阶与 p 互素. 因此存在某个 K-轨道, 其阶与 p 互素. 设 O 为元素 as 的 K-轨道. 用 H' 表示 as 在 G 作用下的稳定子 aHa^{-1}. 则 as 在 K 的限制作用下的稳定子显然是 $H'\cap K$, 且指标 $[K:H'\cap K]$ 是 $|O|$, 它与 p 互素. 又由于它是 H 的共轭, 因而 H' 是 p-群. 因此 $H'\cap K$ 是 p-群. 由此得到 $H'\cap K$ 是 K 的西罗子群. ■

西罗第三定理的证明 由推论(4.7), G 的所有西罗子群都共轭于给定的某一个, 比如说 H. 因而西罗子群的个数是 $s=[G:N]$, 其中 N 是 H 的正规化子. 因为 $H\subset N$, $[G:N]$ 整除 $[G:H]=m$. 要证 $s\equiv 1$(模 p), 我们将西罗子群的集合 $\{H_1,\cdots,H_s\}$ 分解为 $H=H_1$ 共轭作用的轨道. 一个轨道由单独一个群 H_i 组成当且仅当 H 包含在 H_i 的正规化子 N_i 之中. 如果这样, 则 H 和 H_i 都是 N_i 的西罗子群, 且 H_i 在 N_i 中正规. 推论(4.7b)表明 $H=H_i$. 因而只有一条阶为 1 的 H-轨道, 即 $\{H\}$. 其余的轨道有能被 p 整除的阶, 因为由计数公式, 它们的阶整除 $|H|$. 这证明了 $s\equiv 1$(模 p). ■ 208

第五节 12 阶 群

本节我们用西罗定理对 12 阶群分类:

【5.1】定理 *存在 5 个 12 阶群的同构类. 它们的代表是:*

(i) *循环群的直积* $C_3\times C_4$;

(ii) *循环群的直积* $C_2\times C_2\times C_3$;

(iii) *交错群* A_4;

(iv) *二面体群* D_6;

(v) *由* x, y *生成的群, 满足关系* $x^4=1$, $y^3=1$, $xy=y^2x$.

注意 $C_3\times C_4$ 同构于 C_{12}, 而 $C_2\times C_2\times C_3$ 同构于 $C_2\times C_6$[第二章(8.4)].

证明 设 G 是 12 阶群. 用 H 记 G 的一个西罗 2-子群, 它的阶为 4, 用 K 记一个西罗 3-子群, 它的阶为 3. 由定理(4.8)得到西罗 2-子群的个数是 1 或 3, 而西罗 3-子群的个数是 1 或 4. 此外, H 是 4 阶群因而它要么是循环群要么是克莱因四元群 V, 即两个 2 阶循环群的直积:

【5.2】 $$H\approx C_4 \quad 或 \quad H\approx V.$$

【5.3】引理 *两个子群* H, K *中至少有一个是正规的.*

证明 设 K 不正规. 则 K 有四个共轭子群 $K=K_1,\cdots,K_4$. 因为 $|K_i|=3$, 这些群中任

意两个的交必为单位元. 数一下 G 的元素表明只有 3 个元素不在群 K_i 的任何一个之中.

任意西罗 2-子群的阶为 4，且 $H\cap K_i=\{1\}$. 因而它由这 3 个元素加上单位元 1 组成. 这刻画了 H 并表明只存在一个西罗 2-子群. 这样 H 是正规的. ■

209

因为 $H\cap K=\{1\}$，HK 的每个元素都可以唯一地写为乘积 hk[第二章(8.6)]的形式，且由于 $|G|=12$，因此 $HK=G$. 如果 H 正规，则 K 通过共轭在 H 上作用，我们将证明这个作用与 H 和 K 的结构一起确定 G 的结构. 类似地，若 K 正规，则 H 在 K 上作用，且这个作用确定 G.

情形 1：H 和 K 都正规. 则由第二章(8.6)，G 同构于积群 $H\times K$. 由(5.2)，存在两种可能：

【5.4】 $$G\approx C_4\times C_3 \quad 或 \quad G\approx V\times C_3.$$

这些是 12 阶阿贝尔群.

情形 2：H 正规但 K 不正规. 则存在 4 个共轭的西罗 3-子群$\{K_1,\cdots,K_4\}$，且 G 以共轭作用在这 4 个子群的集合 S 上. 这一作用确定一个置换表示

【5.5】 $$G\xrightarrow{\varphi}S_4.$$

我们证明这时 φ 将 G 同构地映到交错群 A_4 上.

K_i 关于共轭作用的稳定子是正规化子 $N(K_i)$，它包含 K_i. 计数公式表明 $|N(K_i)|=3$，因而 $N(K_i)=K_i$. 由于子群 K_i 仅有的公共元素是单位元，因此只有单位元稳定所有这些子群. 这样 φ 是单射且 G 同构于它在 S_4 中的象.

因为 G 有 4 个 3 阶子群，它含有 8 个 3 阶元素，且这些元素当然生成群. 若 x 阶为 3，则 $\varphi(x)$ 是 S_4 中的一个 3 阶置换. 3 阶置换是偶的. 因而 $\mathrm{im}\varphi\subset A_4$. 因为 $|G|=|A_4|$，所以两个群相等.

作为推论，我们注意到如果 H 正规但 K 不正规，则 H 是克莱因四元群 V，这是因为 A_4 的西罗 2-子群是 V.

情形 3：K 正规但 H 不正规. 这一情形中 H 通过共轭在 K 上作用，且由 H 的一个元素作的共轭是 K 的自同构. 我们令 y 是循环群 K 的生成元：$y^3=1$. K 上只存在两个自同构，即恒等映射和交换 y 和 y^2 的自同构.

假设 H 是 4 阶循环群，并令 x 生成 H：$x^4=1$. 则由于 G 不是阿贝尔群，$xy\neq yx$，因而 x 作的共轭不是 K 的平凡同构. 所以 $xyx^{-1}=y^2$. 托特–柯克斯特尔算法(见第九节)是一个证明这些关系定义一个 12 阶群的方法：

【5.6】 $$x^4=1,\quad y^3=1,\quad xyx^{-1}=y^2.$$

最后一种可能性是 H 同构于克莱因四元群. 由于 K 只有两个自同构，因而存在除了单位元以外的元素 $w\in H$，它平凡地作用：$wyw^{-1}=y$. 由于 G 是非阿贝尔群，因而还存在元素 v，它非平凡地作用：$vyv^{-1}=y^2$. 于是 H 的元素是$\{1, v, w, vw\}$，关系 $v^2=w^2=1$ 和 $vw=wv$ 在 H 中成立. 元素 $x=wy$ 的阶为 6，而 $vxv^{-1}=vwyv^{-1}=wy^2=y^2w=x^{-1}$. 关系 $x^6=1$，$v^2=1$，$vxv^{-1}=x^{-1}$定义了群 D_6，故这种情形中 G 是二面体群. 210

第六节 对称群计算

关于置换计算要注意两点. 第一点涉及乘法的顺序. 为了有一个一致的约定，我们用函数记号 $p(x)$表示所有的映射 p，包括置换. 这样，乘积 pq 应该解释为合成作用 $p\circ q$，即“先用 q 然后用 p 作用.”当进行置换乘法时，更为常见的是将 pq 视为“先用 p 然后用 q 作用.”我们这里用的是第二个约定. 要使置换 p 与在指标 i 上作用的记号相容，需要将置换写在指标的右边：

$$(i)p.$$

先用 p 然后用 q 作用到指标 i 上，我们得到$((i)p)q=(i)pq$，这正是所要的. 实际上，这个记号看起来有些古怪. 我们通常省去括号而记为

$$(i)p=ip.$$

重要的是 p 必须放在右边.

为了使对乘法的约定与矩阵乘法相容，必须将第一章(4.6)中 p 的相应的矩阵 P 用其转置 P^t 代替，并用它从右边乘行向量.

要注意的第二点是，用置换矩阵计算并不方便，因为相对于它所包含的信息量来说，矩阵太大了. 需要一个更好的记号. 描述置换的一个方法是用表. 可考虑将排列

【6.1】 $$p=\begin{bmatrix}1&2&3&4&5&6&7&8\\4&6&8&3&5&2&1&7\end{bmatrix}$$

作为由

$$1p=4,\quad 2p=6,\cdots$$

定义的置换的记号. 使用这个记号很容易计算乘积. 例如，若

$$q=\begin{bmatrix}1&2&3&4&5&6&7&8\\2&4&6&8&1&3&5&7\end{bmatrix},$$

则可以把两个表接起来算出 pq(先 p 后 q)的值：

$$pq=\begin{bmatrix}1&2&3&4&5&6&7&8\\8&3&7&6&1&4&2&5\end{bmatrix}.$$

表(6.1)要写的仍然很多，当然，顶行总是相同的. 原则上可将其省去而将要写的数量减半，但如果要置换如18个那样多个数字时，则会很难在底行找到位置. 211

另一个很常用的记号，称为*循环记号*，它最多用 n 个符号描述一个 n 元置换，并且它是基于将指标划分为置换的作用的轨道这一事实. 设 p 是一个置换，并设 H 是 p 所生成的循环群. 我们将集合$\{1, \cdots, n\}$分解成 H-轨道并将这些轨道称为 p-轨道. p-轨道构成指标集合的划分，

称为关于置换 p 的循环分解.

如果一个指标 i 属于一条有 k 个元素的轨道，则轨道中的元素为

$$O=\{i,ip,ip^2,\cdots,ip^{k-1}\}.$$

我们把 ip^r 记作 i_r，从而 $O=\{i_0, i_1, \cdots, i_{k-1}\}$，则 p 在这一条轨道上的作用如下

【6.2】

$$i_0 \to i_1 \to i_2 \to \cdots \to i_{k-1} \to i_0.$$

一个在指标集的子集$\{i_0, i_1, \cdots, i_{k-1}\}$上如此作用而使剩下的指标不动的置换称为循环置换. 这样

【6.3】

$$\sigma = 1 \to 4 \to 3 \to 8 \to 7 \to 1$$

定义$\{$**1**, …, **8**$\}$的一个 5 阶循环，没有提到的指标 **2**，**5**，**6** 被理解为不动的——它们中的每一个都构成一条一个元素的 σ-轨道. 当我们说*置换作用的指标*时，是指那些不是不动的指标：在这一情形下就是 **1**，**3**，**4**，**7**，**8**.

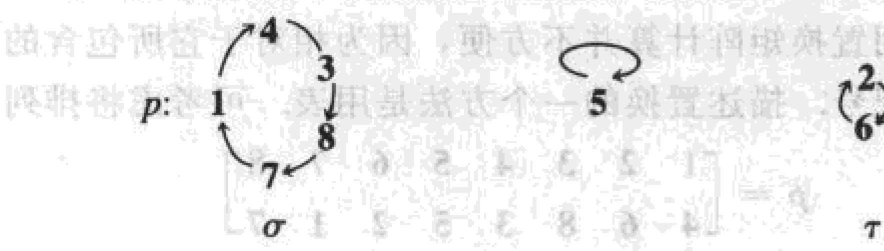
$\{$**1**, …, **8**$\}$的另一个循环置换是

【6.4】

$$\tau = 2 \rightleftarrows 6.$$

这样的 2 阶循环置换称为一个*对换*. 对换是在两个指标上作用的置换.

我们的置换 p(6.1)不是循环的，因为存在三条 p-轨道：



显然有

$$p=\sigma\tau=\tau\sigma,$$

212 其中 $\sigma\tau$ 表示置换的积.

【6.5】命题 设 σ，τ 是作用在互不相交的集合上的置换. 则 $\sigma\tau=\tau\sigma$.

证明 如果 σ 或 τ 都不在一个指标 i 上作用，则 $i\sigma\tau=i\tau\sigma=i$. 若 σ 将 i 变为 $j\neq i$，则 τ 使 i 和 j 都不变. 在这一情形，$i\sigma\tau=j\tau=j$，$i\tau\sigma=i\sigma=j$. 对 τ 在 i 上作用的情形也可同样证明. ■

然而注意，当将作用在重叠指标集上的置换相乘时，作用不一定可交换. 当 $n>2$ 时，对称群 S_n 不是交换群. 例如，若 τ' 是交换 3 和 6 的对换，而 σ 如上，则 $\sigma'\tau\neq\tau\sigma'$.

【6.6】命题 每一个不是恒等的置换 p 是在互不相交的指标集上作用的循环置换的乘积：$p=\sigma_1\sigma_2\cdots\sigma_k$，并且这些循环置换 σ_r 由 p 唯一确定.

证明 我们知道，当限制在单独一条轨道上时，p 的作用为循环置换. 对每一条 p-轨道，可以定义一个循环置换 σ_r，它与 p 以同样的方式置换这条轨道而使其他的指标不变. 显然 p 是

这些循环置换的乘积．反之，设 p 可写成在不同的指标集 O_1，…，O_k 上作用的循环置换的乘积 $\sigma_1\cdots\sigma_k$．根据命题(6.5)，与顺序没有关系．注意 σ_2，…，σ_k 保持 O_1 的元素不动；因此 p 和 σ_1 在 O_1 上以同样的方式作用．因此 O_1 是一条 p-轨道．对其他的循环置换有同样的结果．这样 O_1，…，O_k 是含有多于一个元素的 p-轨道，而 σ_r 是在证明开始所构造的循环置换．■

循环置换(6.2)的循环记号是

【6.7】

$$(i_0 i_1 \cdots i_{k-1}).$$

这样上面的置换 σ 的循环记号是(**14387**)．记号不是完全由置换决定的，因为可以从任意一个指标 i_0，…，i_{k-1} 开始这个序列．对于 σ 有 5 个等价的记号：

$$\sigma = (\mathbf{43871}) = (\mathbf{38714}) = \cdots.$$

使用这些记号中任何一个都可以．

对于任意一个置换 p，其循环记号可如下得到：将置换写成在不相交的指标集上的循环置换的乘积，然后依次用循环记号写出这些置换．顺序是无关紧要的．这样上面的置换 p 的两个可能的循环记号是

$$(\mathbf{14387})(\mathbf{26}) \quad 和 \quad (\mathbf{62})(\mathbf{87143}).$$

如果愿意的话，可以加上"1-循环"(**5**)来表示不动的元素 **5**，这样所有的指标都出现在序列中．但这不符合惯例．

213

有了这个记号，每个置换都可以用最多 n 个整数的串通过适当加括号来表示．乘积仍可通过并置来刻画．上面的置换 q 的循环记号是(**124875**)(**36**)．这样

【6.8】

$$pq = \overset{\sigma}{(\mathbf{14387})}\overset{\tau}{(\mathbf{26})}\overset{\sigma'}{(\mathbf{124875})}\overset{\tau'}{(\mathbf{36})} = \sigma\tau\sigma'\tau'.$$

这一串循环代表置换 pq．要计算积在一个指标上的取值，跟随在 4 个因子之后的指标就是：

$$1 \overset{\sigma}{\rightsquigarrow} 4 \overset{\tau}{\rightsquigarrow} 4 \overset{\sigma'}{\rightsquigarrow} 8 \overset{\tau'}{\rightsquigarrow} 8, 等等.$$

然而(6.8)没有显示 pq 分解为不相交的循环，因为有些指标出现多次．如上的置换计算给出循环分解

$$pq = (\mathbf{185})(\mathbf{237})(\mathbf{46}) =$$

计算完成后，每个指标最多出现一次．

另一个例子，设 $\rho = (\mathbf{548})$．则

【6.9】

$$\sigma\rho = (\mathbf{14387})(\mathbf{548}) = (\mathbf{187})(\mathbf{345})$$

$$\rho\sigma = (\mathbf{548})(\mathbf{14387}) = (\mathbf{147})(\mathbf{385}).$$

现在我们计算置换 p 的共轭．因为 p 是不相交循环的积，只要描述一个循环置换 σ(比如置换$(i_1\cdots i_k)$)的共轭 $q^{-1}\sigma q$ 就够了．(我们交换了乘积顺序这一事实使得 q^{-1} 的共轭的表达式比 q 的要稍微好一些．)

【6.10】命题

(a) 设 σ 表示循环置换$(i_1 i_2 \cdots i_k)$，并设 q 是任意置换．用 j_r 表示指标 $i_r q$．则共轭置换 $q^{-1}\sigma q$ 是循环置换$(j_1 j_2 \cdots j_k)$．

(b) 如果将任意置换 p 写为不相交循环 σ 的积，则 $q^{-1}pq$ 是不相交循环 $q^{-1}\sigma q$ 的积.

(c) 两个置换 p，p' 是对称群的共轭元素当且仅当它们的循环分解有相同的阶.

证明 (a)的证明由下面的计算得到：

$$j_r q^{-1}\sigma q = i_r \sigma q = i_{r+1} q = j_{r+1},$$

其中指标要模 k 理解. (b)容易得到. 此外，由(b)得到共轭置换有相同阶的循环分解. 反过来，设 p 和 p' 是阶都相同的循环分解. 比如说 $p=(i_1\cdots i_r)(i'_1\cdots i'_s)\cdots$ 而 $p'=(j_1\cdots j_r)(j'_1\cdots j'_s)\cdots$. 定义 q 是使 $i_v \rightsquigarrow j_v$，$i'_v \rightsquigarrow j'_v$，等等的置换. 则 $p'=q^{-1}pq$. ■

作为一个例子，我们确定对称群 S_4 的类方程. 这个群有 6 个对换

$$(12),\ (13),\ (14),\ (23),\ (24),\ (34),$$

3 个不相交对换的积

$$(12)(34),\ (13)(24),\ (14)(23),$$

8 个 3-循环和 6 个 4-循环. 由命题(6.10)，这些集合中每一个构成一个共轭类. 因而 S_4 的类方程为

$$24 = 1 + 3 + 6 + 6 + 8.$$

我们现在将刻画对称群 S_p 的子群 G，它的阶被 p 整除而它的西罗 p-子群是正规的. 假设 p 是素整数. 因为 p 只整除 $p! = |S_p|$ 一次，它也只整除 G 一次，因而 G 的西罗 p-子群是循环群.

这样的子群用有限域 $\mathbb{F}_p$ 有一个的非常好的刻画. 对此，我们用有限域的元素 $\{\mathbf{0}, \mathbf{1}, \cdots, \boldsymbol{p-1}\}$ 作为指标. 这个集合的一些置换由域在自身上的作用给出. 即对任意给定的 a，$c\in\mathbb{F}_p$，$c\neq 0$，有作用(加上 a)和(乘以 c). 它们是可逆的作用，因而是 $\mathbb{F}_p$ 的置换，从而它们代表对称群的元素. 例如，(加上 1)是 p-循环

【6.11】
$$(\text{加上 }1) = (\mathbf{012}\cdots(\boldsymbol{p-1})).$$

算子(乘以 c)总是使指标 $\mathbf{0}$ 不动，但其循环分解依赖于 $\mathbb{F}_p^{\times}$ 中元素 c 的阶. 例如，

【6.12】
$$\begin{aligned}(\text{乘以 }2) &= (\mathbf{1234}) \quad \text{如果 } p = 5\\ &= (\mathbf{124})(\mathbf{365}) \text{ 如果 } p = 7.\end{aligned}$$

结合加法和乘法作用给出了 $\mathbb{F}_p$ 上形如

【6.13】
$$x \rightsquigarrow cx + a$$

的所有算子. 这些算子的集合构成对称群的一个 $p(p-1)$ 阶的子群 G.

算子(6.3)的群有一个很好的矩阵表示，可表示为元素在域 $\mathbb{F}_p$ 中且形如

【6.14】
$$\begin{bmatrix}1 & a\\ & c\end{bmatrix}$$

的矩阵的集合. 矩阵通过右乘作用于向量$(1, x)$，将它变为$(1, cx+a)$. 这样可以通过在右边乘上相应的矩阵而重新得到 G 在 $\mathbb{F}_p$ 上的作用. (用右乘是由于对作用顺序的选择.)作用(加上 a)和(乘以 c)由下列的初等矩阵代表：

$$\begin{bmatrix}1 & a\\ & 1\end{bmatrix},\ \begin{bmatrix}1 & \\ & c\end{bmatrix}.$$

【6.15】定理 设 p 是素数，H 是对称群 S_p 的阶被 p 整除的子群. 若 H 的西罗 p-子群正规，则通过对指标适当地编号，H 包含在形如(6.13)的算子群中.

例如，二面体群 D_p 在一个正 p 边形的顶点上忠实地作用，因而可以实现为对称群 S_p 的一个子群．它是(6.14)由 $c=\pm1$ 的矩阵组成的子群．

定理的证明 S_p 仅有的 p 阶元素是 p-循环．因而 H 包含一个 p-循环，设为 σ．我们可以给指标标号使 σ 成为一个标准 p-循环(加上 1)$=(\mathbf{01}\cdots(\boldsymbol{p-1}))$．则这个置换生成 H 的西罗 p-子群．

设 τ_1 是 H 的另一个元素．我们需要证明 τ_1 对应一个形如(6.13)的算子．比如 τ_1 使指标 $\mathbf{0}$ 变到 $\boldsymbol{i}$．因为 σ^i 也将 $\mathbf{0}$ 变到 $\boldsymbol{i}$，所以积 $\tau=\sigma^{-i}\tau_1$ 使 $\mathbf{0}$ 不变．只要证明 τ 具有(6.13)的形式即可，为此，我们将证明 τ 是算子(乘以 c)中的一个．

由假设，$K=\{1,\ \sigma,\ \cdots,\ \sigma^{p-1}\}$ 是 H 的一个正规子群．因而对某个介于 1 与 $p-1$ 之间的 k

【6.16】
$$\tau^{-1}\sigma\tau=\sigma^k$$

成立．我们现在计算这个等式的两边来确定 τ．由命题(6.10)，左边是 p-循环 $\tau^{-1}\sigma\tau=(\mathbf{0}\,\tau\ \mathbf{1}\,\tau\cdots(\boldsymbol{p-1})\tau)$，而直接计算右边得到 $\sigma^k=(\mathbf{0}\boldsymbol{k}\ \mathbf{2}\boldsymbol{k}\cdots(\boldsymbol{p-1})\boldsymbol{k})$：

$$(\mathbf{0}\,\tau\ \mathbf{1}\,\tau\cdots(\boldsymbol{p}-\mathbf{1})\,\tau)=(\mathbf{0}\boldsymbol{k}\ \mathbf{2}\boldsymbol{k}\cdots(\boldsymbol{p}-\mathbf{1})\boldsymbol{k}).$$

必须对这两个循环的相等性仔细地加以解释，这是因为循环记号不是唯一的．我们需要知道左边的第一个指标与右边的第一个指标相等．不然的话就需要确定两个循环中相等的指标并从它们开始．这就是为什么要由正规化开始来得到 $\mathbf{0}\,\tau=\mathbf{0}$．由此，两个序列是相同的，我们得到

$$\mathbf{1}\,\tau=\boldsymbol{k},\mathbf{2}\,\tau=\mathbf{2}\boldsymbol{k},\cdots.$$

这就是算子(乘以 k)，正好是我们所断言的． ■

现在暂时转到作用的顺序问题．如果希望在这一节使用记号 $p(\mathbf{i})$ 表示置换，如在其他地方对函数所使用的一样，就必须相应地修正计算循环的方式．最系统的方法是把包括循环在内的所有东西都从右到左地读．具体地讲，应该把循环(**14387**)理解为

$$\mathbf{1}\leftarrow\!\!\!\sim\mathbf{4}\leftarrow\!\!\!\sim\mathbf{3}\leftarrow\!\!\!\sim\mathbf{8}\leftarrow\!\!\!\sim\mathbf{7}\leftarrow\!\!\!\sim\mathbf{1}.$$

这是置换(6.3)的逆．可以把乘积(**14387**)(**548**)解释为合成："先用(**548**)作用，然后用(**14387**)作用"．计算这个乘积得出

$$\mathbf{1}\leftarrow\!\!\!\sim\mathbf{8}\leftarrow\!\!\!\sim\mathbf{7}\leftarrow\!\!\!\sim\mathbf{1},\quad \mathbf{3}\leftarrow\!\!\!\sim\mathbf{5}\leftarrow\!\!\!\sim\mathbf{4}\leftarrow\!\!\!\sim\mathbf{3},$$

我们将其写作(**187**)(**354**)．注意这里得到与(6.9)同样的符号串．令人称奇的是，当我们作置换乘法时，把所有的东西都往回读得到同样的答案．当然，现在记号(**187**)(**354**)表示的是置换(6.9)的逆．

第七节 自 由 群

我们看到一些群，如对称群 S_3、二面体群 D_n 以及平面刚体运动群 M，可以通过一系列的生成元和关系来处理它们而使得很容易进行计算．本章剩下的部分将讨论这种方法的形式上的背景．在本节中，我们考虑有生成元集合的群，除了由群的公理所给出的那些关系[如 $x(yz)=(xy)z$]外，这些群不满足任何其他关系．群的元素的一个集合 S 称为*自由的*，如果其元素除了群的公理给出的关系外不满足任何别的关系，具有自由的生成元集合的群称为*自由群*．我们现在就刻画自由群．

我们从符号的任意一个集合 S 开始，比如 $S=\{a,\ b,\ c,\ \cdots\}$，它可以有限也可以无限，

定义一个字为 S 中符号的一个允许重复的有限串．例如 a，aa，ba 和 $aaba$ 为字．两个字可以通过并置合成：

$$aa, ba \rightsquigarrow aaba.$$

这样所有字的集合 W 有一个合成的结合律．此外，可以引入“空字”作为这个法则的单位元．我们需要一个符号表示空字；就用 1 吧．集合 W 称为符号集合 S 上的**自由半群**．不幸的是它不是一个群，因为没有逆元素，而逆元素的引入是一件复杂的事情．

设 S' 是由 S 中的符号以及符号 $a^{-1}(a \in S)$ 组成的集合：

【7.1】
$$S' = \{a, a^{-1}, b, b^{-1}, c, c^{-1}, \cdots\}.$$

217 设 W' 是用 S' 中符号构成的字的集合．如果对于某个 x，一个字 $w \in W'$ 看起来是

$$\cdots xx^{-1}\cdots \quad \text{或} \quad \cdots x^{-1}x\cdots,$$

则我们可以约定消去两个符号 x，x^{-1} 以缩短字的长度．不能这样消去的字称为**约化字**．从任意字 w 开始，可以作一有限序列的消去而最终得到约化字 w_0，它也可能会是空字 1．我们把这个字 w_0 称为 w 的**约化型**．

常常会有不止一种方式进行消去．例如，从 $w = babb^{-1}a^{-1}c^{-1}ca$ 开始，可以有多种消去方式，如

$$\begin{array}{cc}
\underline{ba}\,\cancel{b}\cancel{b}^{-1}a^{-1}c^{-1}c\,\underline{a} & \underline{ba}bb^{-1}a^{-1}\cancel{c}^{-1}\cancel{c}a \\
\downarrow & \downarrow \\
\underline{b}\,\cancel{a}\cancel{a}^{-1}c^{-1}c\,\underline{a} & \underline{ba}bb^{-1}\cancel{a}^{-1}\cancel{a} \\
\downarrow & \downarrow \\
\underline{b}\,\cancel{c}^{-1}\cancel{c}\,\underline{a} & \underline{ba}\,\cancel{b}\cancel{b}^{-1} \\
\downarrow & \downarrow \\
ba & ba.
\end{array}$$

最后得到相同的约化字，虽然其字母来自原来的字的不同位置．（下划线的字母是最后剩下的字母．）这是一般的情形．

【7.2】命题 一个给定的字 w 只有一个约化型．

证明 对字 w 的长度作归纳．如果 w 是约化的，则没有什么需要证明．否则，必存在可以消去的字母对，比如说，下面的下划线对

$$w = \cdots \underline{xx^{-1}}\cdots.$$

（我们用 x 表示 S' 中的任意元素，并且按照明显的约定，如果 $x = a^{-1}$ 则 $x^{-1} = a$．）如果证明了通过先消去对 $\underline{xx^{-1}}$ 就可得到 w 的每一个约化型 w_0，则在这样得到的较短的字 $\cdots \cancel{x}\cancel{x}^{-1}\cdots$ 上用归纳法便得到命题．

设 w_0 是 w 的一个约化型，我们知道 w_0 是由 w 通过一系列消去得到的．第一种情形是对在这个过程序列中的某一步被消去．则也可以重新安排其顺序而首先消去 $\underline{xx^{-1}}$．因而这种情形已经解决了．另一方面，因为 w_0 是约化的，对 $\underline{xx^{-1}}$ 不会保留在 w_0 中．因而两个符号中至少有一个在某个时候被消去．如果对本身没有被消去，则涉及对的第一个消去必为

$$\cdots \cancel{x}^{-1}\underline{\cancel{x}x^{-1}}\cdots \quad \text{或} \quad \cdots \underline{x\cancel{x}^{-1}}\,\cancel{x}\cdots.$$

注意到由这个消去得到的字与通过消去原来的对$\underline{xx^{-1}}$得到的字是一样的. 因而可以在这一步用消去原来的对来代替. 这使我们回到第一种情形，命题得证. ■ [218]

我们称W'中的两个字w，w'是等价的，并写作$w\sim w'$，如果它们有相同的约化型. 这是一个等价关系.

【7.3】命题 等价的字的乘积是等价的：若$w\sim w'$且$v\sim v'$，则$wv\sim w'v'$.

证明 要得到等价于乘积wv的约化字，可首先将w和v中的字母对尽可能多地消去，从而将w约化为w_0，v约化为v_0. 于是wv约化为w_0v_0. 现在如果有可能，我们继续约化w_0v_0. 因为$w\sim w'$和$v\sim v'$，同样的过程用于$w'v'$，也需经过w_0v_0，从而给出同样的约化字. ■

由命题得到字的等价类可以做乘积，即在字的等价类的集合上面有一个唯一定义的合成法则.

【7.4】命题 令F表示W'中字的等价类的集合. 则F关于W'导出的合成法则是一个群.

证明 乘法是结合的和空字1的类是单位元这两个事实由W'中的相应事实得到. 还需验证F的所有元素可逆. 但显然，如果$w=xy\cdots z$，则$z^{-1}\cdots x^{-1}y^{-1}$的类是类$w$的逆. ■

【7.5】定义 字的等价类的群F称为集合S上的自由群.

因而由命题(7.2)，自由群F的一个元素恰好对应于W'的一个约化字. 要乘约化字，先组合然后再消去：

$$(abc^{-1})(cb) \rightsquigarrow abc^{-1}cb = abb.$$

对约化字也可以引入幂记号：$aaab^{-1}b^{-1}=a^3b^{-2}$.

由一个元素组成的集合$S=\{a\}$上的自由群与所有a的幂的集合$F=\{a^n\}$是相同的. 它是无限循环群，与之相比，两个元素的集合$S=\{a, b\}$上的自由群是非常复杂的.

第八节 生成元与关系

描述了自由群后，我们现在考虑更为可能出现的情形，即群的生成元的集合不是自由的——它们中存在一些非平凡的关系. 我们的讨论基于自由群和商群的映射性质. [219]

【8.1】命题 自由群的映射性质：设F是一个集合$S=\{a, b, \cdots\}$上的自由群，并设G是一个群. 每个集合的映射$f: S\longrightarrow G$以唯一的方式扩张成一个群同态$\varphi: F\longrightarrow G$. 如果把元素$x\in S$的象$f(x)$记为$\tilde{x}$，则$\varphi$将$S'=\{a, a^{-1}, b, b^{-1}, \cdots\}$的一个字映为$G$中元素$\{\tilde{a}, \tilde{a}^{-1}, \tilde{b}, \tilde{b}^{-1}, \cdots\}$的对应的乘积.

证明 这一法则的确定义了S'上字的集合的映射. 我们要证明等价的字映到G中同一个乘积. 但因为字中的消去不改变G中对应的乘积，这是显而易见的. 还有，因为F中的乘法是由并置定义的，这样定义的映射φ是一个同态. 这是f扩张为同态的仅有的方法. ■

如果S是群G的任一子集，则映射性质定义了一个由S上的自由群到G的同态$\varphi: F\rightarrow G$. 这反映出在F中除了由群的公理推出的关系外S的元素不满足别的关系，并且解释了形容词自由的原因.

说一个元素簇S生成群G，如果从S的自由群到G的映射φ是满射. 这与说G中每一个元素都是S'的某个元素串的乘积是一样的，因此它与第二章第二节所引入的术语是一致的. 在任何情况下，无论S是否生成G，命题(8.1)中的同态的象都是一个子群，称为由S生成的

子群. 这个子群恰好由 S'的元素的所有乘积构成.

设 S 生成G. 则 S 的元素称为生成元. 因为 φ 是满同态，第一同构定理[第二章(10.9)]告诉我们 G 同构于商群 F/N，其中 $N=\ker\varphi$. N 中的元素称为生成元间的关系. 它们是在 G 中对应的积为 1 的字 w 的等价类：

$$\varphi(w)=1 \quad \text{或} \quad \text{在} G \text{中有} w=1.$$

在 $N=\{1\}$的特殊情形时，φ 是同构. 此时，G 也叫做自由群.

如果知道一个生成元的集合并且还知道所有的关系，则可以在同构的群 F/N 中从而也能在群 G 中进行计算. 但除非 G 是自由的，否则子群 N 是无限的，所以我们不能列出它的所有元素. 更准确地说，字的集合

$$R=\{r_1,r_2,\cdots\}$$

称为 G 的一个定义关系的集合，如果 $R\subset N$ 并且 N 是包含 R 的最小的正规子群. 这表明 N 是由它的一个包含 R 中的所有字及其所有共轭的子集合生成的.

要求定义关系是群 N 的生成元可能看起来更为完整. 但记住由一个生成元集合定义的同态 $F\longrightarrow G$ 的核总是正规子群，因而没有必要使定义关系列得更长. 如果知道某个关系 $r=1$ 在 G 中成立，则只需在等式的两边简单地左乘 g 右乘 g^{-1} 即可得到 $grg^{-1}=1$ 在 G 中亦成立.

220

我们已经知道一些生成元和关系的例子，如二面体群 D_n[第五章(3.6)，(3.7)]. 它由两个元素 x，y 生成，满足关系

【8.2】 $$x^n=1,\quad y^2=1,\quad xyxy=1.$$

【8.3】命题 元素 x^n，y^2，$xyxy$ 构成二面体群的一个定义关系的集合.

这个命题实质上在第五章(3.6)就已验证过. 但要正式证明它，以及要自由地使用生成元和关系的概念，就需要所谓的商群的映射性质. 它是第一同构定理的一个推广：

【8.4】命题 商群的映射性质：设 N 是群 G 的正规子群，设$\overline{G}=G/N$，并设 π 是由 $\pi(a)=\overline{a}=aN$ 定义的典范映射 $G\longrightarrow\overline{G}$. 令 $\varphi:\overline{G}\longrightarrow G'$是一个其核包含 N 的同态. 存在唯一同态 $\overline{\varphi}$ 使得 $\overline{\varphi}\pi=\varphi$：

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\overline{\varphi}} & \\ & \overline{G} & \end{array}$$

这个映射由规则 $\overline{\varphi}(\overline{a})=\varphi(a)$定义.

证明 要定义映射 $\overline{\varphi}$: $\overline{G}\longrightarrow G'$，必须对 $\overline{G}$ 的每一个元素 α 定义 $\overline{\varphi}(\alpha)$. 为此用一个元素 $a\in G$ 来代表 α，选择 a 使得 $\alpha=\pi(a)$. 用上划线的符号，也就是说 $\alpha=\overline{a}$. 既然我们希望映射 $\overline{\varphi}$ 满足关系 $\overline{\varphi}(\pi(a))=\varphi(a)$，那么除了用规则 $\overline{\varphi}(\alpha)=\varphi(a)$来定义 $\overline{\varphi}$ 以外没有别的选择，这正是命题所断言的. 要证这是可行的，必须证我们得到的 $\overline{\varphi}(\alpha)$的值，即 $\varphi(a)$只依赖于 α 而与我们的选择的 a 无关. 这常被称为证明我们的映射是"唯一定义的."

设 a 和 a'是 G 的两个元素，满足$\overline{a}=\overline{a'}=\alpha$. 等式$\overline{a}=\overline{a'}$表明 $aN=a'N$，或 $a'\in aN$[第二章(5.13)]. 于是存在某个 $n\in N$ 使得 $a'=an$. 因为由假设 $N\subset\ker\varphi$，所以 $\varphi(n)=1$. 这样 $\varphi(a')=\varphi(a)\varphi(n)=\varphi(a)$，这正是所要求的.

最后，因为 $\bar{\varphi}(\bar{a})\bar{\varphi}(\bar{b})=\varphi(a)\varphi(b)=\varphi(ab)=\bar{\varphi}(\overline{ab})$，所以映射 $\bar{\varphi}$ 是一个同态. ■

命题(8.3)的证明 在第五章(3.6)我们已证明 D_n 由满足(8.2)的元素 x，y 生成. 因而有一个由 x，y 上的自由群到 D_n 的满射 φ: $F\longrightarrow D_n$，且 $R=\{x^n,\ y^2,\ xyxy\}$包含在 $\ker\varphi$ 中. 设 N 是 F 中包含 R 的最小的正规子群. 则由于 $\ker\varphi$ 是一个包含 R 的正规子群，因此 $N\subset\ker\varphi$. 商群的映射性质给出一个同态 $\bar{\varphi}$: $F/N\longrightarrow D_n$. 若证明 $\bar{\varphi}$ 是一个一一映射，则命题得证.

221

注意由于 φ 是满射，因此 $\bar{\varphi}$ 也是. 并且在 F/N 中，关系 $\bar{x}^n=1$，$\bar{y}^2=1$ 和 $\bar{x}\bar{y}\bar{x}\bar{y}=1$ 成立. 应用这些关系，可将任意 $\bar{x}$，$\bar{y}$ 的字变成 $\bar{x}^i\bar{y}^j$ 的形式，其中 $0\leqslant i\leqslant n-1$ 及 $0\leqslant j\leqslant 1$. 这表明 F/N 最多有 $2n$ 个元素. 由于 $|D_n|=2n$，由此得到 $\bar{\varphi}$ 是一一映射，这正是要证的. ■

我们将用记号

【8.5】
$$\langle x_1,\cdots,x_m;r_1,\cdots,r_k\rangle$$

表示由元素 x_1，…，x_m 生成且满足定义关系 r_1，…，r_k 的群. 这样

【8.6】
$$D_n=\langle x,y;x^n,y^2,xyxy\rangle.$$

作为一个新的例子，考虑由 x，y 生成并满足单独一个关系 $xyx^{-1}y^{-1}=1$ 的群. 如果 x，y 是一个群的元素，则

【8.7】
$$xyx^{-1}y^{-1}$$

称为它们的换位子. 换位子在重要性在于：它等于 1 当且仅当 x 和 y 可交换. 这可以由在等式 $xyx^{-1}y^{-1}=1$ 的两边右乘上 yx 得到. 因此如果在自由群上加上条件 $xyx^{-1}y^{-1}=1$，我们将得到一个群，在这个群中 x 与 y 可交换. 这样如果 N 是包含换位子的最小正规子群并且如果$G=F/N$，则 x 和 y 的剩余是 G 中的交换元素. 这使得 G 中任意两个元素可交换.

【8.8】命题 *设 F 是 x，y 上的自由群而 N 是由换位子 $xyx^{-1}y^{-1}$ 生成的最小正规子群. 则商群 $G=F/N$ 是阿贝尔群.*

证明 我们用同样的字母 x，y 表示 G 中生成元 x，y 的剩余. 由于换位子属于 N，元素 x，y 在 G 中可交换. 于是 x 亦与 y^{-1} 可交换. 因为在左面乘上 y 后，xy^{-1} 和 $y^{-1}x$ 都成为 x. 故由消去律，它们亦相等. 还有，x 显然与 x^{-1} 可交换. 这样 x 与 $S'=\{x,\ x^{-1},\ y,\ y^{-1}\}$中的任一个字可交换. y 也是同样的. 由归纳得到 S'上的任意两个字可交换. 因为 x，y 生成群，所以 G 是可交换的. ■

注意这个结果：S'中的任意两个字的换位子 $uvu^{-1}v^{-1}$ 属于由单个换位子 $xyx^{-1}y^{-1}$ 生成的正规子群，这是因为由于 u，v 在 G 中交换，因而其换位子在 G 中代表单位元.

上面构造的群 G 称为集合$\{x,\ y\}$上的*自由阿贝尔群*，这是因为元素 x，y 不满足除了由群公理及交换律得到的关系外的其他任何关系.

在上面的例子中我们看到，关系的知识使得在群中计算起来非常容易. 这多少是有点误解的，因为用一个给定的关系集合来计算常常一点也不容易. 例如，假定把二面体群的定义关系(8.6)稍微作点改动，用 y^3 来代替 y^2：

222

【8.9】
$$G=\langle x,y;x^n,y^3,xyxy\rangle.$$

这个群就复杂多了. 当 $n>5$ 时，它是个无限群.

当关系太复杂时，问题就变得非常困难. 假设有一个字的集合 R，并设 N 是包含 R 的最

小的正规子群．设 w，w'是任意其他字．则我们可以提出 w 和 w'是否代表 F/N 中的同一个元素这一问题．这称为**群的字问题**，可以知道没有一个能在可预计的时间长度内对其作出决定的一般过程．然而生成元和关系在许多情形下使得我们能够有效地进行计算，因此它们是非常有用的工具．在下一节我们将讨论一种重要的计算方法，即托德-考克斯特算法．

记住当说到由生成元 S 和关系 R 定义的群时，我们是指一个商群 F/N，其中 F 是 S 上的自由群而 N 是 F 中包含 R 的最小的正规子群．注意任意一个关系集合都会定义一个群，因为 F/N 总是有定义的．R 越大，N 就变得越大，在同态 $\pi: F \longrightarrow F/N$ 中发生的坍缩就越大．如果 R"太大了"，可能发生最坏的情形是 $N=F$，从而 F/N 是平凡群．这样不会出现像关系的矛盾集合之类的东西．仅有的问题是在 F/N 变得太小时产生，这时关系会引起比我们所期待的更多的坍缩产生．

第九节 托德-考克斯特算法

设 H 是有限群 G 的一个子群．本节描述的托德-考克斯特算法是一个令人惊叹的计算 H 在 G 中的陪集个数和确定 G 在陪集上作用的直接方法．因为我们知道在轨道上的任意作用看起来都像在陪集上的作用[第五章(6.3)]，该算法实际上是描述任意群作用的．

要具体地进行计算，群 G 和子群 H 都要以具体的方式给出．这样我们考虑一个群

【9.1】
$$G = \langle x_1, \cdots, x_m; r_1, \cdots, r_k \rangle$$

如上节中由生成元 x_1，…，x_m 和具体给出的关系 r_1，…，r_k 表出．这样 G 实现为一个商群 F/N，其中 F 是集合$\{x_1, \cdots, x_m\}$上的自由群而 N 是包含$\{r_1, \cdots, r_k\}$的最小正规子群．我们还假设 G 的子群 H 由一个在自由群 F 中的字的集合

【9.2】
$$\{h_1, \cdots, h_s\}$$

223 具体给出，这个集合在 G 中的象生成 H．

我们从一个特殊的例子开始．将 G 取为由三个元素 x，y，z 生成的群，满足关系 x^3，y^2，z^2，xyz，而把 H 取作由 z 生成的循环群：

【9.3】
$$G = \langle x, y, z; x^3, y^2, z^2, xyz \rangle, \quad H = \{z\}.$$

因为要确定在陪集上的作用，它是置换表示[第五章(8.1)]，我们必须确定如何写出置换．我们将使用第六节的循环记号．这要求使用右陪集 Hg 而不是左陪集，因为希望 G 从右边作用．我们将 H 在 G 中右陪集的集合记作 $\mathscr{C}$．还必须确定如何具体地描述群的作用，最简单的办法是再回到自由群，即描述关于给定生成元 x，y，z 的置换．

生成元在陪集上的作用要满足下面这些规则：

【9.4】规则

1. 每个生成元(我们例子中的 x，y，z)的作用是一个置换．
2. 关系(我们例子中的 x^3，y^2，z^2，xyz)平凡地作用．
3. H 的生成元(我们例子中的 z)使陪集 $H1$ 不动．
4. 在陪集上的作用是可迁的．

第一个规则是群作用的一般性质．它由群元素是可逆的这一事实得到．我们将其列出而不

是明确地提到生成元的逆元素．第二个规则成立是因为在 G 中关系代表 1，且是群 G 在作用．规则 3 和 4 是在陪集上作用的特殊性质．

我们现在只使用这些规则来确定陪集表示．用指标 **1**，**2**，**3**，…表示陪集，用 **1** 代表陪集 $H1$．因为我们不知道有多少陪集，所以不知道需要多少个指标．必要时将加上新的指标．

首先，规则 3 告诉我们 z 将 **1** 映到其自身：$z\mathbf{1}=\mathbf{1}$．这用尽了规则 3 提供的所有信息，然后接着用规则 1 和 2．规则 4 并没有被直接用到．

我们不知道 x 如何在 **1** 上作用．于是猜测 $\mathbf{1}x\neq\mathbf{1}$，并为它指定一个新的指标，比如 $\mathbf{1}x=\mathbf{2}$．继续考虑生成元 x，我们不知道 $\mathbf{2}x$，因而指定第三个指标 $\mathbf{1}x^2=\mathbf{2}x=\mathbf{3}$．规则 2 现在开始起作用．它告诉我们 x^3 使每个指标都不动．因而 $\mathbf{1}x^3=\mathbf{3}x=\mathbf{1}$．习惯上把这些信息综合在一个表

$$\begin{array}{cccc} & x & x & x \\ \hline \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \end{array}$$

之中，它展示了 x 在这三个指标上的作用．关系 xxx 出现在上面，规则 2 反映在同一个指标 **1** 出现在其两端这个事实上．至此，我们已确定了 x 在三个指标 **1**，**2**，**3** 上的作用，只是还不知道这些指标是否代表不同的陪集．

224

现在要求 y 在指标 **1** 上的作用．我们也不知道它，因而为它指定一个新的指标，比如说 $\mathbf{1}y=\mathbf{4}$．再次应用规则 2．因为 y^2 平凡地作用，可知 $\mathbf{1}y^2=\mathbf{4}y=\mathbf{1}$：

$$\begin{array}{ccc} & y & y \\ \hline \mathbf{1} & \mathbf{4} & \mathbf{1}. \end{array}$$

剩下的关系是 xyz．我们知道 $\mathbf{1}x=\mathbf{2}$，但仍不知道 $\mathbf{2}y$，于是令 $\mathbf{1}xy=\mathbf{2}y=\mathbf{5}$．这样规则 2 告诉我们 $\mathbf{1}xyz=\mathbf{5}z=\mathbf{1}$：

$$\begin{array}{cccc} & x & y & z \\ \hline \mathbf{1} & \mathbf{2} & \mathbf{5} & \mathbf{1}. \end{array}$$

现在应用规则 1：每个群元素的作用是指标的一个置换．我们已确定了 $\mathbf{1}\,z=\mathbf{1}$ 以及 $\mathbf{5}z=\mathbf{1}$．从而得到 $\mathbf{5}=\mathbf{1}$．用 **1** 代入消去指标 **5**．这又告诉了我们 $\mathbf{2}y=\mathbf{1}$．另一方面，我们已知道 $\mathbf{4}y=\mathbf{1}$．于是由规则 1 得 $\mathbf{4}=\mathbf{2}$，从而也消去了 **4**．

现在下面表中的元素都已被确定：

	x	x	x	y	y	z	z	x	y	z
1	**2**	**3**	**1**	**2**	**1**	**1**	**1**	**2**	**1**	**1**
2	**3**	**1**	**2**	**1**	**2**		**2**	**3**		**2**
3	**1**	**2**	**3**		**3**		**3**	**1**	**2**	**3**.

右下角表明 $\mathbf{2}z=\mathbf{3}$．这确定了表的其余部分．共有三个指标，而作用为

$$x=(\mathbf{1\,2\,3}),\quad y=(\mathbf{1\,2}),\quad z=(\mathbf{2\,3}).$$

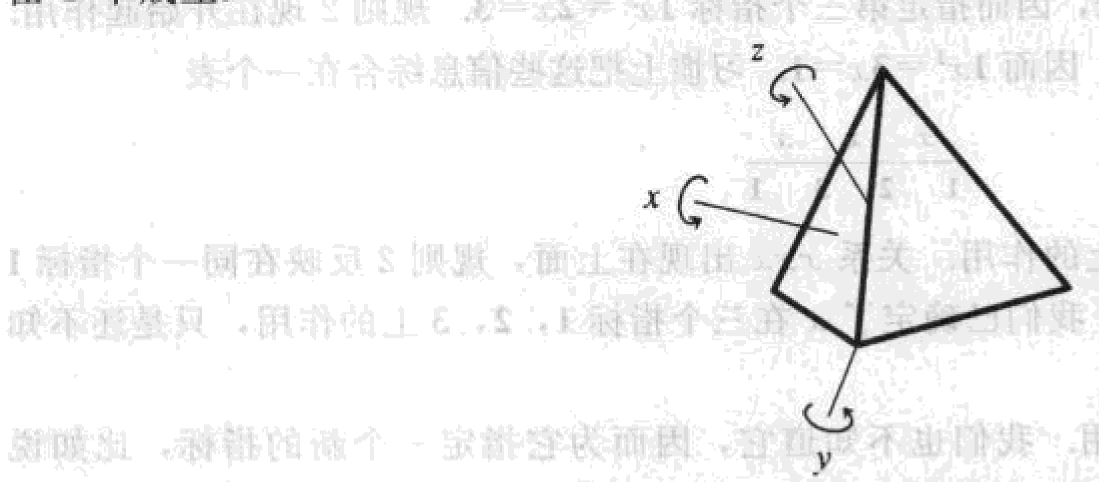
因为有 3 个指标，所以我们推断出存在三个陪集且 H 在 G 中的指标为 3．还可推断出 H 的阶为 2，于是 G 的阶为 6．因为 $z^2=1$ 是我们的关系之一；因而 z 的阶是 1 或 2，又由于 z 在指标上的作用不平凡，因此 $z\neq 1$．上面列出的三个置换生成对称群，因而置换表示是一个从 G 到 S_3 的同构．

当然，这些结果依赖于我们知道所构造的置换表示是正确的．我们将在本节结尾证明这一点．下面再计算几个例子．

【9.5】例 考虑由正四面体的 12 个旋转对称组成的正四面体群 T(见第五章第九节)．如果令 y 和 x 表示绕一个顶点和绕一个面的中心反时针方向转过 $\frac{2\pi}{3}$ 的旋转，如下所示，则 $yx=z$ 为绕一条边转过 π 的旋转．这样关系

225

【9.6】
$$x^3=1,\quad y^3=1,\quad yxyx=1$$
在 T 中成立．



我们证明(9.6)是 T 的关系的完全集合．为此，考虑由这些关系定义的群 $G=\langle y, x; y^3, x^3, yxyx\rangle$．由于关系(9.6)在 T 中成立，商群的映射性质给出了一个同态 $\varphi: G\longrightarrow T$．这个映射是个满射，因为容易看出 y 和 x 生成 T．我们仅需证明 φ 是个单射．这一点将通过证明群 G 的阶为 12 来证明．

可以直接分析关系，但并不特别的容易．我们也可以通过枚举平凡子群 $H=\{1\}$ 的陪集来计算 G 的阶．这也并不有效．最好是用 G 的一个非平凡子群 H，比如由 y 生成的子群．因为 $y^3=1$，这个子群的阶最多为 3．如果证明其阶为 3 而其在 G 中的指标为 4，则将得到 G 的阶为 12，从而可以完成证明．

下面是得到的表．填表的时候从关系的两边开始．

	x	x	x	y	y	y	y	x	y	x
1	2	3	1	1	1	1	1	2	3	1
2	3	1	2	3	4	2	3	1	1	2
3	1	2	3	4	2	3	4	4	2	3
4	4	4	4	2	3	4	2	3	4	4

这样置换表示为

【9.7】
$$x=(\mathbf{123}),\quad y=(\mathbf{234}).$$
因为有 4 个指标，可以 H 的指标为 4．还有，注意 y 的阶的确恰好是 3．因为 $y^3=1$，阶最多为 3，而由于与 y 相应的置换(**234**)的阶为 3，它至少是 3．于是群的阶是 12，这正是我们所预计的．通过验证置换(9.7)生成这个群，可以顺便导出 T 同构于交错群 A_4 这一事实．

226

【9.8】例 我们对关系(9.6)稍微做点改动．设 G 是由 x，y 生成的群，满足关系
$$x^3=1,\quad y^3=1,\quad yxy^2x=1,$$

并设 H 是由 y 生成的子群. 我们这样开始作表. 由于 $y^3=1$，因此用 y^{-1} 代替 y^2 从而缩短关系的长度. 显然，y^{-1} 作为与 y 相应的置换的逆来作用. 从右边做起确定了底行的元素.

	x		x		x		y		y		y		y		x		y^{-1}		x	
1		**2**		**3**		**1**		**1**		**1**		**1**		**1**		**2**		**3**		**1**
2						**2**						**2**		**3**		**1**		**1**		**2**

我们将关系 $\mathbf{2}y^{-1}=\mathbf{3}$ 重新写成 $\mathbf{3}y=\mathbf{2}$. 因为也有 $\mathbf{2}y=\mathbf{3}$，从而得到 $\mathbf{3}y^2=\mathbf{3}$ 及 $\mathbf{3}y^3=\mathbf{2}$. 但 $y^3=1$，于是 $\mathbf{3}=\mathbf{2}$，结果这又蕴涵 $\mathbf{1}=\mathbf{2}=\mathbf{3}$. 因为生成元 x，y 使 1 不动，所以只能有一个陪集，于是$H=G$. 因而 x 是 y 的幂. 第三个关系表明 $x^2=1$. 将这个事实与第一个关系结合起来，我们得到 $x=1$. 这样 G 是 3 阶循环群. 这个例子展示了关系是如何坍缩群的.

在例子中，我们把 H 取作由 G 的选定生成元之一所生成的子群，但也可以用由任意字的集合生成的子群 H 进行计算. 使用规则 3 必定会使得它们进入计算.

当 G 为无限时也可以用这个方法，只要指标$[G:H]$是有限的. 如果有无限多个陪集，则不能指望这个过程会停下来.

现在考虑为什么我们所描述的过程的确给出了陪集上的作用这个问题. 在正式定义算法之前，想要正式地证明这个事实是不可能的，而我们还没有定义算法. 因而将非正式地讨论这个问题. 我们这样来描述计算的过程：在计算的一个特定阶段，有某个指标集合 $\boldsymbol{I}$，且群的某些生成元在一些指标上的作用已被确定. 我们把这称为在 $\boldsymbol{I}$ 上的一个*部分作用*. 一个部分作用不必符合规则 1，2 和 3，但应该是可迁的；即每个指标都应该属于 **1** 的"部分轨道". 这里规则 4 起了作用. 它告诉我们不引入任何我们不需要的指标.

开始的位置是 $\boldsymbol{I}=\{\mathbf{1}\}$，且没有指定的作用. 在任何一个阶段都有两个可能的步骤：

【9.9】

(i) 作为前面三个规则之一的结果，可以等同两个指标 $\boldsymbol{i}$，$\boldsymbol{j}\in\boldsymbol{I}$，或者

(ii) 可以选择一个生成元 x 和一个指标 $\boldsymbol{i}$ 使得 $\boldsymbol{i}x$ 还没有被确定，并且定义 $\boldsymbol{i}x=\boldsymbol{j}$，其中 $\boldsymbol{j}$ 是个新的指标.

当作用都已确定并且它们符合我们的规则，即当得到一个完全的、没有冲突的表格并且所有规则都成立时，就中止过程.

存在两个问题：第一，这个过程会中止吗？第二，如果它中止，作用是否是正解？两个问题的答案都是肯定的. 可以证明如果群有限且优先进行步骤(i)，则这个过程总是会中止的. 我们不去证明这一点. 对于应用来讲，更为重要的事实是如果过程终止，则结果得到的置换表示是正确的.

【9.10】定理 *假设经过有限次反复使用步骤(i)和(ii)得到一个没有冲突的表. 则这个表定义一个置换表示，并且通过适当地标号，它同构于陪集表示.*

证明的概述 用 $\boldsymbol{I}^*$ 表示最后得到的带有作用的指标集合. 我们将通过定义一个由这个集合到陪集的集合的与两个作用相容的一一映射 φ^*：$\boldsymbol{I}^*\longrightarrow\mathscr{C}$来证明命题. 我们归纳地定义 φ^*：在每一阶段定义一个由在该阶段所确定的指标集合到$\mathscr{C}$的映射 $\varphi:\boldsymbol{I}\longrightarrow\mathscr{C}$，使得映射 φ 与 $\boldsymbol{I}$ 上的部分作用相容. 开始时，$\{\mathbf{1}\}\longrightarrow\mathscr{C}$使得 $\mathbf{1}\rightsquigarrow H1$. 现假设 $\varphi:\boldsymbol{I}\longrightarrow\mathscr{C}$已经定义，并设 $\boldsymbol{I}'$

228

227

是在 $\boldsymbol{I}$ 上应用步骤(9.9)之一的结果. 在步骤(ii)的情形不难将 φ 拓广为一个映射 φ': $\boldsymbol{I}'\longrightarrow\mathscr{C}$. 当$k\neq j$ 时定义 $\varphi'(k)=\varphi(k)$而定义 $\varphi'(j)=\varphi(i)x$. 其次，假设用步骤(i)使两个指标相同，比如说 i, j，则 $\boldsymbol{I}$ 被坍缩而构成一个新的指标集合 $\boldsymbol{I}'$. 下面的引理使我们能够定义映射 φ': $\boldsymbol{I}'\longrightarrow\mathscr{C}$:

【9.11】引理 假设给定一个与 $\boldsymbol{I}$ 上的部分作用相容的映射 $\varphi:\boldsymbol{I}\longrightarrow\mathscr{C}$，设 i, $j\in\boldsymbol{I}$ 并且假定规则 1，2 或 3 之一使得 $i=j$. 则 $\varphi(i)=\varphi(j)$.

证明 这是对的，因为我们已注意到陪集上的作用的确满足(9.4)的所有规则. 因而如果规则使得 $i=j$，它们也使得 $\varphi(i)=\varphi(j)$. ■

还需要证明映射 φ^*：$\boldsymbol{I}^*\longrightarrow\mathscr{C}$是一一映射. 为此，我们使用下面的引理构造逆映射 ψ^*：$\mathscr{C}\longrightarrow\boldsymbol{I}^*$.

【9.12】引理 设 S 是一个 G 在其上作用的集合，并假设 $s\in S$ 是一个被 H 稳定的元素. 存在唯一的与在两个集合上的作用相容的映射 ψ: $\mathscr{C}\longrightarrow S$ 使得 $H1 \rightsquigarrow s$.

证明 除了这里改为右作用以外，证明是第五章(6.4)的重复. 由于 g 使得 $H\rightsquigarrow Hg$ 且我们希望 $\psi(Hg)=\psi(H)g$，因此必须取 $\psi(Hg)=sg$. 这证明了映射 ψ 的唯一性. 要证存在性，我们首先验证规则 $\psi(Hg)=sg$ 是唯一定义的：如果 $Ha=Hb$，则 $ba^{-1}\in H$. 由假定，ba^{-1}稳定 s，从而 $sa=sb$. 最后，因为 $\psi(Hga)=sga=(sg)a=\psi(Hg)a$，所以 ψ 与G 的作用相容. ■

228

要证 φ^* 的双射性，我们现在用这个引理构造一个映射 ψ^*：$\mathscr{C}\longrightarrow\boldsymbol{I}^*$. 考虑合成映射 $\varphi^*\psi^*$：$\mathscr{C}\longrightarrow\mathscr{C}$，它使得 $H1\rightsquigarrow H1$. 再次应用引理，以$\mathscr{C}$代替 S. 引理的唯一性告诉我们 $\varphi^*\psi^*$是恒等映射. 另一方面，因为 $\boldsymbol{I}^*$ 上的作用是可迁的并且由于 ψ^* 与作用相容，ψ^* 必为满射. 由此得 φ^* 和 ψ^* 都是一一映射. ■

公理化方法与直接做相比有许多优势.

Bertrand Russell

练　习

第一节　群在自身的作用

1. 规则 g, $x\rightsquigarrow xg^{-1}$是否定义一个 G 在自身的作用?
2. 设 H 是群 G 的子群. 则 H 以左乘在 G 上作用. 刻画这个作用的轨道.
3. 证明公式 $|G|=|Z|+\sum|C|$，其中和号指在含有多于一个元素的共轭类上取和，而 Z 是G 的中心.
4. 证明不动点定理(1.12).
5. 在平面运动群 M 中确定共轭类.
6. 在下列各式中尽可能多地划去那些 10 阶群的类方程：
   $1+1+1+2+5$，$1+2+2+5$，$1+2+3+4$，$1+1+2+2+2+2$.
7. 设 $F=\mathbb{F}_5$. 确定 $GL_2(\mathbb{F}_5)$中$\begin{bmatrix}1 & \\ & 2\end{bmatrix}$的共轭类的阶.
8. 确定下面每个群的类方程.
   (a) 四元数群　(b) 克莱因四元群　(c) 二面体群 D_5　(d) D_6
   (e) D_n　(f) $GL_2(\mathbb{F}_3)$中的上三角矩阵群　(g) $SL_2(\mathbb{F}_3)$
9. 设 G是一个 n 阶群而 F 是任意域. 证明 G同构于$GL_n(F)$的子群.

10. 求下列每个矩阵在 $GL_3(\mathbb{R})$ 中的中心化子.

(a) $\begin{bmatrix}1&&\\&2&\\&&3\end{bmatrix}$ (b) $\begin{bmatrix}1&&\\&1&\\&&2\end{bmatrix}$ (c) $\begin{bmatrix}1&1&\\&1&\\&&1\end{bmatrix}$ (d) $\begin{bmatrix}1&1&\\&1&1\\&&1\end{bmatrix}$ (e) $\begin{bmatrix}1&&\\&&1\\&1&\end{bmatrix}$ (f) $\begin{bmatrix}&1&\\&&1\\1&&\end{bmatrix}$

*11. 确定所有至多有三个共轭类的有限群.

12. 设 N 是群 G 的一个正规子群. 假设 $|N|=5$ 且 $|G|$ 是奇数. 证明 N 含于 G 的中心.

*13. (a) 确定 8 阶群可能的类方程.

(b) 给出 8 阶群的分类.

14. 设 Z 是群 G 的中心. 证明如果 G/Z 是循环群, 则 G 是阿贝尔群, 因而 $G=Z$.

*15. 设 G 是 35 阶群.

(a) 设 G 在五个元素的集合上非平凡地作用. 证明 G 有一个 7 阶正规子群.

(b) 证明每个 35 阶群都是循环群.

第二节 二十面体群的类方程

1. 对如图(2.7)所示的正八面体和正方体确定交 $I\cap O$.
2. 两个正四面体可内接到一个正方体中, 每个使用其一半顶点. 将这一事实与包含关系 $A_4\subset D_4$ 联系起来.
3. I 是否包含一个子群 T ? D_6? D_3?
4. 证明二十面体群没有 30 阶子群.
5. 证明或推翻: A_5 是 S_5 仅有的真正规子群.
6. 证明当 p 为素数且 $e>1$ 时, 没有 p^e 阶的单群.
7. 证明或推翻: 阿贝尔群是单群当且仅当它的阶为素数.
8. (a) 确定正四面体旋转群 T 的类方程.

   (b) T 的中心是什么?

   (c) 证明 T 恰有一个 4 阶子群.

   (d) 证明 T 没有 6 阶子群.
9. (a) 确定正八面体群 O 的类方程.

   (b) O 恰有两个真正规子群. 求出它们, 并证明它们正规且没有其他正规子群.
10. 证明四面体群 T 同构于交错群 A_4, 而正八面体群 O 同构于对称群 S_4. 从求这些群作用的一个四元素集合开始.
11. 证明或推翻: 二十面体群不是实上三角 2×2 矩阵群的子群.

*12. 证明或推翻: 非阿贝尔单群不能在含有少于五个元素的集合上非平凡地作用.

第三节 在子集上的作用

1. 设 S 是二面体群 D_3 的 2 阶子集的集合. 确定 D_3 在 S 上共轭作用的轨道.
2. 确定左乘和共轭作用在 D_3 的 3 阶子集上的轨道.
3. 列出二面体群 D_4 的所有子群, 并将其分为共轭类.
4. 设 H 是群 G 的子群. 证明在共轭作用下左陪集 gH 的轨道包含右陪集 Hg.
5. 设 U 是有限群 G 的子集, 并设 $|U|$ 和 $|G|$ 没有公因子. 在共轭作用下 U 的稳定子平凡吗?
6. 考虑 G 在其子集的集合上的左乘作用. 设 U 是一个子集, 它的轨道 $\{gU\}$ 划分 G. 设 H 是这条轨道中包含 1 的唯一子集. 证明 H 是 G 的子群而集合 gU 是其左陪集.
7. 设 H 是群 G 的子群. 证明或推翻: 正规化子 $N(H)$ 是 G 的一个正规子群.
8. 设 $H\subset K\subset G$ 是群. 证明 H 在 K 中正规当且仅当 $K\subset N(H)$.
9. 证明 $GL_n(\mathbb{R})$ 的上三角矩阵的子群 B 与下三角矩阵的子群 L 共轭.

10. 设 B 是 $G=GL_n(\mathbb{C})$ 的上三角矩阵子群，并设 $U\subset B$ 是对角元素为 1 的上三角矩阵的集合. 证明 $B=N(U)$ 且 $B=N(B)$.

*11. 用 S_n 表示 $GL_n(\mathbb{R})$ 的置换矩阵子群. 确定 S_n 在 $GL_n(\mathbb{R})$ 中的正规化子.

12. 设 S 是有限集合，群 G 在其上可迁地作用，并且设 U 是 S 的子集. 证明了集 gU 均匀地覆盖 S，即 S 的每个元素在同样多个集合 gU 中.

13. (a) 设 H 是 G 的一个 2 阶正规子群. 证明 H 在 G 的中心中.

(b) 设 H 是有限群 G 的一个素数 p 阶正规子群. 假设 p 是整除 $|G|$ 的最小素数. 证明 H 属于中心 $Z(G)$.

*14. 设 H 是有限群 G 的一个真子群. 证明 H 的共轭的并不是整个群 G.

15. 设 K 是群 G 的一个 2 阶正规子群，且设 $\overline{G}=G/K$. 设 $\overline{C}$ 是 $\overline{G}$ 的一个共轭类. 设 S 是 $\overline{C}$ 在 G 中的逆象. 证明下列两种情形之一成立.

(a) $S=C$ 是单独一个共轭类且 $|C|=2|\overline{C}|$.

(b) $S=C_1\cup C_2$ 由两个共轭类组成且 $|C_1|=|C_2|=|\overline{C}|$.

16. 计算二面体群 D_n 的子群 $H=\langle 1, y\rangle$ 的双陪集 HgH. 证明每个双陪集中有两个或四个元素.

17. 设 H，K 是 G 的子群，H' 是 H 的一个共轭子群. 建立双陪集 $H'gK$ 和 HgK 间的联系.

18. 关于双陪集 HgK 的阶有什么结论？

第四节 西罗定理

1. 20 阶群中含有多少个 5 阶元？

2. 证明没有 pq 阶的单群，其中 p，q 是素数.

3. 证明没有 p^2q 阶的单群，其中 p，q 是素数.

4. 证明矩阵 $\begin{bmatrix}1 & a\\ & c\end{bmatrix}$ 的集合(其中 a，$c\in\mathbb{F}_7$ 且 $c=1, 2, 4$)构成(4.9b)中表出的群(因而这样的群存在).

5. 在下列情形求西罗 2-子群：

(a) D_{10} (b) T (c) O (d) I.

6. 求 $GL_2(\mathbb{F}_p)$ 的西罗 p-子群.

*7. (a) 设 H 是群 G 的素数 p 阶子群. H 的共轭子群的个数可能是什么？

231

(b) 设 p 是整除 $|G|$ 的最小素数. 证明 H 是正规子群.

*8. 设 H 是 G 的西罗 p-子群，并设 $K=N(H)$. 证明或反证：$K=N(K)$.

9. 设 G 是 $p^e m$ 阶群. 证明对每个整数 $r\leqslant e$，G 含有 p^r 阶子群.

10. 设 $n=pm$ 是恰为被 p 整除一次的一个整数，并且设 G 是一个 n 阶群. 设 H 是 G 的西罗 p-子群，且设 S 是所有西罗 p-子群的集合. S 如何分解为 H-轨道？

*11. (a) 求 $GL_n(\mathbb{F}_p)$ 的阶.

(b) 求 $GL_n(\mathbb{F}_p)$ 的一个西罗 p-子群.

(c) 求西罗 p-子群的个数.

(d) 用西罗第二定理给出西罗第一定理的另一个证明.

*12. 证明没有 224 阶单群.

13. 证明如果 G 的阶为 $n=p^e a$，其中 $1\leqslant a<p$ 且 $e\geqslant 1$，则 G 有一个真正规子群.

14. 证明阶 <60 的单群仅有素数阶的.

15. 将 33 阶群分类.

16. 将 18 阶群分类.

17. 证明最多只有五个 20 阶群的同构类.

*18. 设 G 是 60 阶单群.

(a) 证明 G 含有六个西罗 5-子群、十个西罗 3-子群和五个西罗 2-子群.

(b) 证明 G 同构于交错群 A_5.

第五节　12 阶群

1. 求所有 12 阶群的类方程.
2. 证明 $n=2p$ 阶群是循环群或二面体群，其中 p 是素数.

*3. 设 G 是 30 阶群.

(a) 证明西罗 5-子群 H 或西罗 3-子群 K 是正规的.

(b) 证明 HK 是 G 的一个循环子群.

(c) 将 30 阶群分类.

4. 设 G 是 55 阶群.

(a) 证明 G 由两个元素 x，y 生成，关系为 $x^{11}=1$，$y^5=1$，$yxy^{-1}=x^r$，其中 $1\leqslant r<11$.

(b) 证明下列 r 值是不可能的：2，6，7，8，10.

(c) 证明其余的值都可能，而且存在两个 55 阶群的同构类.

第六节　对称群计算

1. 验证积(6.9).
2. 直接证明置换$(\mathbf{123})(\mathbf{45})$与$(\mathbf{241})(\mathbf{35})$共轭.
3. 设 p，q 是置换. 证明 pq 与 qp 有同样大小的循环.
4. (a) 对称群 S_7 是否有 5 阶元？10 阶元？15 阶元？

(b) S_7 的元素最大可能的阶是多少？

5. 当一个置换写成循环的积时，说明如何确定它的奇偶性.
6. 证明或推翻：置换的阶是构成它的循环的阶的最小公倍数.
7. S_n 的由循环$(\mathbf{12345})$生成的循环子群 H 是否是正规子群.

*8. 计算 S_n 中不使任意指标不动的置换的个数.

9. 求置换 $i \rightsquigarrow n-i$ 的循环分解.
10. (a) 证明每个置换 p 是对换的乘积.

(b) 写出循环$(\mathbf{123}\cdots \mathbf{n})$需要多少个对换？

(c) 设置换有两种写为对换乘积的方法，比如 $p=\tau_1\tau_2\cdots\tau_m$ 和 $p=\tau_1'\tau_2'\cdots\tau_n'$. 证明 m 和 n 同为奇或同为偶.

11. 元素$(\mathbf{12})$在 S_4 中的中心化子是什么？
12. 求对称群 S_4 的所有 4 阶子群. 哪些是正规的？
13. 确定 A_4 的类方程.
14. (a) 确定 S_5 的共轭类的个数并求其类方程.

(b) 列出 A_5 的共轭类，并将它与二十面体群的共轭类的列表[见(2.2)]对应起来.

15. 证明对换$(\mathbf{12})$，$(\mathbf{23})$，…，$(\mathbf{n-1},\mathbf{n})$生成对称群 S_n.
16. 证明对称群 S_n 由循环$(\mathbf{12}\cdots \mathbf{n})$和$(\mathbf{12})$生成.
17. (a) 证明两个对换的积$(ij)(kl)$总可写为 3-循环的积. 同时考虑某些指标相同的情形.

(b) 证明如果 $n\geqslant 3$，交错群 A_n 由 3-循环生成.

18. 证明 S_n 的包含一个 3-循环的真的正规子群是 A_n.

*19. 证明当 $n\geqslant 5$ 时 A_n 是单群.

*20. 证明 A_n 是 S_n 中仅有的指标为 2 的子群.

232

21. 用反群(第二章第一节练习 12)的语言解释本节结尾处令人惊讶的等同的结果.

第七节　自由群

1. 证明或推翻：两个生成元的自由群同构于两个无限循环群的积.
2. (a) 设 F 是 x，y 上的自由群. 证明两个元素 $u=x^2$ 和 $v=y^3$ 生成 F 的一个子群，它同构于 u，v 上的自由群.

   (b) 证明三个元素 $u=x^2$，$v=y^2$ 和 $z=xy$ 生成 F 的一个子群，它同构于 u，v，z 上的自由群.
3. 可以定义 S' 的闭字为一个通过将字的两端连起来得到的有向圈.

$$\begin{matrix} & & c\,a^{-1} & & \\ & b & & b^{-1} & \\ a & & & & b, \\ & a & & c & \\ & & bbd & & \end{matrix}$$

233

当顺时针读时，代表一个闭字. 建立约化闭字与自由群的共轭类的一个一一对应.

4. 设 p 是素数. 令 N 是有限集 S 上长度为 p 的字的个数. 证明 N 被 p 整除.

第八节　生成元与关系

1. 证明群的两个元素 a，b 与 bab^2，bab^3 生成同一个子群.
2. 证明群 G 的包含子集 S 的最小正规子群是由集合 $\{gsg^{-1} \mid g\in G,\ s\in S\}$ 生成的子群.
3. 证明或推翻：y^2x^2 属于由 xy 及其共轭生成的正规子群.
4. 证明由 x，y，z 生成的满足单独关系 $yxyz^{-2}=1$ 的群实际上是自由群.
5. 设 S 是群 G 的元素的集合，并设 $\{r_i\}$ 是在 G 的元素 S 中满足的关系. 设 F 是 S 上的自由群. 证明映射 $F\longrightarrow G$(8.1)通过 F/N 分解，其中 N 是由 $\{r_i\}$ 生成的正规子群.
6. 设 G 是具有正规子群 N 的群. 假设 G 和 G/N 都是循环群. 证明 G 可由两个元素生成.
7. G 的子群 H 称为特征子群，如果它被 G 的所有自同构映为其自身.

   (a) 证明每个特征子群是正规的.

   (b) 证明群 G 的中心 Z 是特征子群.

   (c) 证明由 G 的所有 n 阶元素生成的子群 H 是特征子群.
8. 确定四元数群的正规子群与特征子群.
9. 群 G 的换位子子群 C 是包含所有换位子的最小子群.

   (a) 证明换位子子群是特征子群.

   (b) 证明 G/C 是阿贝尔群.
10. 确定平面运动群 M 的换位子子群.
11. 通过直接计算证明换位子 $x(yz)x^{-1}(yz)^{-1}$ 属于由两个换位子 $xyx^{-1}y^{-1}$ 和 $xzx^{-1}z^{-1}$ 及其共轭生成的正规子群.
12. 用 G 表示(8.8)中定义的自由阿贝尔群 $\langle x, y;\ xyx^{-1}y^{-1}\rangle$. 证明这个群的泛性质：如果 u，v 是一个阿贝尔群 A 的元素，则存在唯一的同态 $\varphi: G\longrightarrow A$，使得 $\varphi(x)=u$ 而 $\varphi(y)=v$.
13. 证明自由群 $\langle x, y\rangle$ 中由单独一个换位子 $xyx^{-1}y^{-1}$ 生成的正规子群是换位子子群.
14. 设 N 是群 G 的一个正规子群. 证明 G/N 是阿贝尔群当且仅当 N 包含 G 的换位子子群.
15. 设 $\varphi: G\longrightarrow G'$ 是群的满同态. 设 S 是 G 的子集，使得 $\varphi(S)$ 是 G' 的生成元，并且设 T 是 $\ker\varphi$ 的生成元集. 证明 $S\cup T$ 生成 G.
16. 证明或推翻：每个有限群 G 可由有限生成元集和有限关系集表出.
17. 设 G 是由 x，y，z 生成的群，满足关系 $\{r_i\}$. 假设关系中的一个具有形式 wx，其中 w 是 y，z 的一个字. 设 r_i' 是通过在 r_i 中用 w^{-1} 代替 x 得到的关系，并设 G' 是由 y，z 生成的、满足关系 $\{r_i'\}$ 的群. 证明 G 与 G' 同构.

234

第九节 托德-考克斯特算法

1. 证明(9.5)的元素 x，y 生成 T，而置换(9.7)生成 A_4.
2. 用托德-考克斯特算法确定由两个元素 x，y 生成的群，关系如下：
   (a) $x^2=y^2=1$，$xyx=yxy$
   (b) $x^2=y^3=1$，$xyx=yxy$
   (c) $x^3=y^3=1$，$xyx=yxy$
   (d) $x^4=y^2=1$，$xyx=yxy$
   (e) $x^4=y^4=x^2y^2=1$
3. 用托德-考克斯特算法确定由两个元素 x，y 生成的群的阶，关系如下.
   (a) $x^4=1$，$y^3=1$，$xy=y^2x$　(b) $x^7=1$，$y^3=1$，$yx=x^2y$
4. 确定由元素 x，y，z 生成且关系为 $x^4=y^4=z^3=x^2z^2=1$ 和 $z=xy$ 的群 G.
5. 分析由 x，y 生成且满足关系 $x^4=1$，$y^4=1$，$x^2=y^2$，$xy=y^3x$ 的群 G.
*6. 分析由元素 x，y 生成的群，满足关系 $x^{-1}yx=y^{-1}$，$y^{-1}xy=x^{-1}$.
7. 设 G 是由元素 x，y 生成且满足关系 $x^4=1$，$y^3=1$，$x^2=yxy$ 的群. 用下面两种方法证明这个群是平凡的.
   (a) 利用托德-考克斯特算法证明.
   (b) 直接用关系证明.
8. 确定由两个元素 x，y 生成且满足关系 $x^3=y^3=yxyxy=1$ 的群 G.
9. 设 $p\leqslant q\leqslant r$ 为 >1 的整数. 三角群 G^{pqr} 由生成元定义 $G^{pqr}=\langle x, y, z; x^p, y^q, z^r, xyz\rangle$. 在下列每一情形证明三角群同构于下列的群.
   (a) 当 p，q，$r=2$，2，n 时，二面体群 D_n
   (b) 当 p，q，$r=2$，3，3 时，四面体群
   (c) 当 p，q，$r=2$，3，4 时，八面体群
   (d) 当 p，q，$r=2$，3，5 时，二十面体群
10. 用 Δ 表示一个等腰直角三角形，且用 a，b，c 表示关于 Δ 的三条边的平面的反射. 设 $x=ab$，$y=bc$，$z=ca$. 证明 x，y，z 生成三角群.
11. (a) 证明由元素 x，y，z 生成且满足关系 $x^2=y^3=z^5=1$，$xyz=1$ 的群 G 的阶为 60.
    (b) 设 H 是由 x 及 zyz^{-1} 生成的子群. 确定 G 在 G/H 上的置换表示，并确定 H.
    (c) 证明 G 同构于交错群 A_5.
    (d) 设 K 是 G 的由 x 及 yxz 生成的子群. 确定 G 在 G/K 上的置换表示，并确定 H.

杂题

1. (a) 证明 O_3 的由正四面体的包括反向对称在内的所有对称构成的子群 T' 的阶为 24.
   (b) T' 同构于对称群 S_4 吗？
   (c) 对于八面体的对称的群叙述并证明类似的结论.
2. (a) 设 $U=\{1, x\}$ 是群 G 的一个 2 阶子集. 考虑下面的图：对 G 的每个元素有一个顶点且对所有 $g\in G$ 有一条连接顶点 g 到 gx 的边. 证明连接顶点 1 的顶点是由 x 生成的循环群的元素.
   (b) 对 $U=\{1, x, y\}$ 做同样的证明.
*3. (a) 设群 G 可迁地作用于集合 S 上，而 H 是一个元素 $s_0\in S$ 的稳定子. 考虑 G 在 $S\times S$ 上由 $g(s_1, s_2)=(gs_1, gs_2)$ 定义的作用. 建立 H 在 G 中的双陪集与 $S\times S$ 中 G-轨道的一个一一对应.
   (b) 对 G 是二面体群 D_5 而 S 是一个五边形的顶点的情形具体给出这个对应.
   (c) 在 $G=T$ 而 S 是正四面体的边的集合时给出这个对应.

235

*4. 设 $H\subset K\subset G$ 是子群，H 是 K 的正规子群而 K 是 G 的正规子群. 证明或推翻：H 在 G 中正规.

*5. 证明布吕阿分解，它断言 $GL_n(\mathbb{R})$ 是双陪集 BPB 的并，其中 B 是上三角矩阵的群而 P 是一个置换矩阵.

6. (a) 用两种方法证明由 x，y 生成的满足关系 x^2，y^2 的群是无限群：

   (i) 显然利用这些关系每个字可以约化为$\cdots xyxy\cdots$的形式. 证明 G 的每个元素恰好由一个这样的字代表.

   (ii) 将 G 表示为由关于其夹角不是 2π 的有理数倍的直线 ℓ，ℓ' 的反射 r，r' 生成的群.

   (b) 设 N 是 G 的任意真的正规子群. 证明 G/N 是二面体群.

7. 设 H，N 是 G 的子群，并设 N 是正规子群.

   (a) 确定典范同态 π：$G\longrightarrow G/N$ 在子群 H 和 NH 上限制的核.

   (b) 应用这些限制条件下的第一同态定理证明第二同构定理：$H/(H\cap N)$同构于$(HN)/N$.

8. 设 H，N 是 G 的正规子群且 $H\supset N$，令 $\overline{H}=H/N$，$\overline{G}=G/N$.

   (a) 证明 $\overline{H}$ 是 $\overline{G}$ 的正规子群.

   236

   (b) 利用合成同态 $G\longrightarrow\overline{G}\longrightarrow\overline{G}/\overline{H}$ 证明第三同构定理：G/H 同构于 $\overline{G}/\overline{H}$.

第七章　双线性型

我认为公式对于无经验的人是冷漠和不受欢迎的.

Benjamin Pierce

第一节　双线性型的定义

我们的双线性型的模型是在第四章第五节中所描述的$\mathbb{R}^n$中向量的点积

【1.1】
$$(X\cdot Y)=X^tY=x_1y_1+\cdots+x_ny_n.$$

符号$(X\cdot Y)$有着许多性质，对于我们来说最重要的是下面这些：

【1.2】

双线性：
$$(X_1+X_2\cdot Y)=(X_1\cdot Y)+(X_2\cdot Y)$$
$$(X\cdot Y_1+Y_2)=(X\cdot Y_1)+(X\cdot Y_2)$$
$$(cX\cdot Y)=c(X\cdot Y)=(X\cdot cY)$$

对称性：
$$(X\cdot Y)=(Y\cdot X)$$

正性：
$$(X\cdot X)>0,\quad \text{如果 } X\neq 0.$$

注意这里的双线性是指：如果固定一个变量，则得到的关于另一个变量的函数是一个线性变换$\mathbb{R}^n\longrightarrow\mathbb{R}$.

本章将学习点积及其类似. 如何将双线性和对称性推广到任意域上的向量空间是清楚的，而正性只能在标量域是实数$\mathbb{R}$时才能使用. 我们将在第四节把正性概念也拓广到复向量空间.

237

设V是域F上的向量空间. V上的一个双线性型是V上的一个有两个变量的在域中取值的函数：$V\times V\xrightarrow{f}F$，满足双线性公理：

【1.3】
$$f(v_1+v_2,w)=f(v_1,w)+f(v_2,w)$$
$$f(cv,w)=cf(v,w)$$
$$f(v,w_1+w_2)=f(v,w_1)+f(v,w_2)$$
$$f(v,cw)=cf(v,w)$$

对所有v，w，v_i，$w_i\in V$和所有$c\in F$成立. 常使用记号

【1.4】
$$\langle v,w\rangle$$

表示型的值$f(v,\ w)$. 因此$\langle v,\ w\rangle$是标量，也就是F中的元素.

一个型$\langle,\rangle$称为对称的，如果对所有v，$w\in V$有

【1.5】
$$\langle v,w\rangle=\langle w,v\rangle,$$

而称为斜对称的，如果对所有v，$w\in V$有

【1.6】
$$\langle v,w\rangle=-\langle w,v\rangle.$$

(如果域F的特征为2，即在F中$1+1=0$时，这实际上不是斜对称的正确定义，我们将在第八节更正定义.)

如果型f是对称的或斜对称的，则第二个变量的线性性可由第一个变量的线性性得到.

双线性型的主要例子是列向量空间F^n上如下得到的型：设A是F上的$n\times n$矩阵，定义

【1.7】
$$\langle X,Y\rangle = X^{t}AY.$$
注意这个积是一个1×1矩阵，也就是一个标量，并且它是双线性的．通常的点积作为$A=I$的情形而被包括在里面．

矩阵A称为对称的，如果

【1.8】
$$A^{t}=A,\quad \text{即对所有 } i,j \text{ 有}\quad a_{ij}=a_{ji}.$$

【1.9】命题 型(1.7)是对称的当且仅当矩阵A是对称的．

证明 设A是对称的．因为$Y^{t}AX$是1×1矩阵，它等于其转置：$Y^{t}AX=(Y^{t}AX)^{t}=X^{t}A^{t}Y=X^{t}AY$．这样$\langle X,Y\rangle=\langle Y,X\rangle$．另一边的论证可通过令$X=e_i$和$Y=e_j$得到．我们有$\langle e_i,e_j\rangle=e_i^{t}Ae_j=a_{ij}$，而$\langle e_j,e_i\rangle=a_{ji}$．如果型是对称的，则$a_{ij}=a_{ji}$，因而$A$是对称的．■

238

设$\langle\,,\rangle$是向量空间V上的一个双线性型，并设$\boldsymbol{B}=(v_1,\cdots,v_n)$是$V$的一个基，通过关于这个基的型的矩阵可以将型与积$X^{t}AY$联系起来．由定义，这个矩阵是$A=(a_{ij})$，其中

【1.10】
$$a_{ij}=\langle v_i,v_j\rangle.$$
注意A是对称矩阵当且仅当$\langle\,,\rangle$是对称型．而且双线性型的对称性与基无关．因而如果型关于一个基的矩阵是对称的，则它关于任意其他基的矩阵亦是对称的．

由矩阵A可计算在任意两个向量$v,w\in V$上型的取值．如第三章第四节一样，设X,Y是这两个向量的坐标向量，则有$v=\boldsymbol{B}X$，$w=\boldsymbol{B}Y$．于是
$$\langle v,w\rangle=\left\langle \sum_i v_i x_i,\sum_j v_j y_j\right\rangle.$$
利用双线性将它展开成为$\sum_{i,j}x_i y_j\langle v_i,v_j\rangle=\sum_{i,j}x_i a_{ij}y_j=X^{t}AY$：

【1.11】
$$\langle v,w\rangle=X^{t}AY.$$
这样，如果像第三章(4.14)那样利用基$\boldsymbol{B}$将F^n与V等同起来，则双线性型$\langle\,,\rangle$对应于$X^{t}AY$．

与线性算子的研究一样，一个中心的问题是描述基变换对这样的积的影响．例如，我们希望知道当$\mathbb{R}^n$的基改变时，点积会变成什么．基变换$\boldsymbol{B}=\boldsymbol{B}'P$在型的矩阵上的影响容易由规则$X'=PX$，$Y'=PY$确定：如果$A'$是型关于新的基$\boldsymbol{B}'$的矩阵，则由$A'$的定义，$\langle v,w\rangle=X'^{t}A'Y'=X^{t}P^{t}A'PY$．但我们还有$\langle v,w\rangle=X^{t}AY$．于是

【1.12】
$$P^{t}A'P=A.$$

令$Q=(P^{-1})^{t}$．因为P可取任意可逆矩阵，所以Q也是任意的．

【1.13】推论 设A是双线性型关于一个基的矩阵．代表同一个型的关于不同基的矩阵A'是矩阵$A'=QAQ^{t}$，其中Q是$GL_n(F)$中的任意矩阵．

现在将公式(1.12)用于$\mathbb{R}^n$中点积的例子．关于标准基点积的矩阵是恒等矩阵：$(X\cdot Y)=X^{t}IY$．于是公式(1.12)告诉我们如果改变基，则型的矩阵变为

【1.14】
$$A'=(P^{-1})^{t}I(P^{-1})=(P^{-1})^{t}(P^{-1}),$$
其中P如同前面一样是基变换矩阵．若矩阵P碰巧是正交的，也就是说$P^{t}P=I$，则有$A'=I$，如我们在第四章(5.13)所看到的，点积变为了点积：$(X\cdot Y)=(PX\cdot PY)=(X'\cdot Y')$．但在一般的基变换下，点积的公式变为$X'^{t}A'Y'$，其中$A'$如(1.14)给出．例如，令$n=2$并且令基$\boldsymbol{B}'$为

239

$$v_1' = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad 和 \quad v_2' = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

则

【1.15】
$$P^{-1} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad 且 \quad A' = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

关于基 $\mathbf{B}'$，矩阵 A' 代表 $\mathbb{R}^2$ 的点积.

也可以把计算反过来. 假设给定实向量空间 V 上的一个双线性型 $\langle , \rangle$. 我们要问是否可以选择适当的基使这个型变为点积. 我们从一个任意的基 $\boldsymbol{B}$ 开始，这样就得到一个用来作为起始的矩阵 A. 于是问题成为是否能以某种方式改变基而使新的矩阵是恒等矩阵. 应用公式(1.12)，这相当于解矩阵方程 $I = (P^{-1})^t A (P^{-1})$，或

【1.16】
$$A = P^t P.$$

【1.17】推论 *代表一个等价于点积的型的矩阵是 $A = P^t P$，其中 P 可逆.*

这个推论给出了一个确定与点积等价的双线性型的问题的理论上的答案，但它并不太令人满意，因为我们还没有一个确定哪些矩阵能够写成乘积 $P^t P$ 的实用的方法，更不要说求 P 的实用的方法了.

由(1.2)所列的点积的性质我们可以得到一些关于矩阵 A 的条件. 双线性性没有给 A 加上任何条件，因为 $X^t A Y$ 总是双线性的. 然而，对称性和正性限制了其可能性. 对称性较为容易验证：要代表点积，矩阵 A 必须是对称的. 正性也是一个强限制. 要代表点积，矩阵 A 必须具有性质

【1.18】
$$对所有\ X \neq 0, 有\ X^t A X > 0.$$

具有这一性质的实对称矩阵称为是*正定的*.

【1.19】定理 *实 $n \times n$ 矩阵 A 的下列性质是等价的：*

(i) 关于 $\mathbb{R}^n$ 的某个基，A 代表点积.

(ii) 存在可逆矩阵 $P \in GL_n(\mathbb{R})$ 使得 $A = P^t P$.

(iii) A 是对称的和正定的.

我们已看到(i)和(ii)是等价的[推论(1.17)]以及(i)蕴涵(iii). 还需证明剩下的(iii)蕴涵(i). 将这个蕴涵用向量空间的形式重新叙述更为方便.

有限维实空间 V 上的对称双线性型 $\langle , \rangle$ 称为*正定的*，如果对每个非零向量 $v \in V$ 有

【1.20】
$$\langle v, v \rangle > 0.$$

这样实对称矩阵 A 是正定的当且仅当它在 $\mathbb{R}^n$ 上定义的型 $\langle X, Y \rangle = X^t A Y$ 为正定型. 而且型 $\langle , \rangle$ 是正定的当且仅当它的关于任意基的矩阵是正定矩阵. 这是显然的，因为如果 X 是向量 v 的坐标向量，则 $\langle v, v \rangle = X^t A X$(1.11).

两个向量 v, w 称为关于一个对称型是*正交的*，如果 $\langle v, w \rangle = 0$. 两个向量的正交性通常记作

【1.21】
$$v \perp w.$$

这个定义拓广了我们已知的当型为 $\mathbb{R}^n$ 的点积时的正交概念[第四章(5.12)]. V 的一个基 $\boldsymbol{B} = (v_1, \cdots, v_n)$ 称为关于型的*标准正交基*，如果

$$对所有\ i \neq j\ 有\ \langle v_i, v_j \rangle = 0, 且对所有\ i\ 有\ \langle v_i, v_i \rangle = 1.$$

240

由定义直接得到一个基 **B** 是标准正交的当且仅当这个型关于 **B** 的矩阵是单位矩阵.

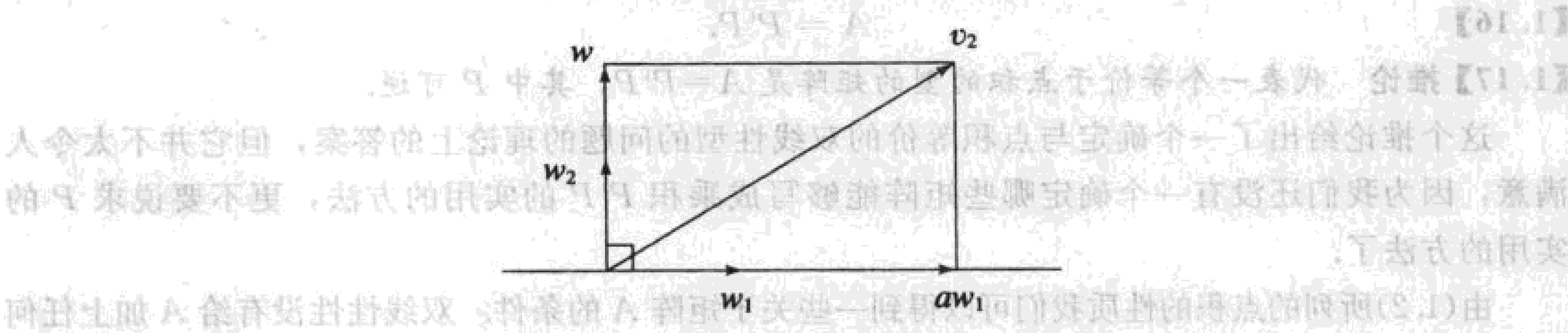
【1.22】定理　设$\langle\ ,\ \rangle$是有限维实向量空间 V 上的正定对称型. 存在 V 的一个标准正交基.

证明　我们将描述一个从任意基 $\mathbf{B}=\{v_1, \cdots, v_n\}$开始构造一个标准正交基的过程，称为格拉姆-施密特过程. 第一步是正规化 v_1，使得$\langle v_1, v_1\rangle=1$. 为此，我们注意到

【1.23】
$$\langle cv, cv\rangle = c^2 v.$$

因为型是正定的，$\langle v_1, v_1\rangle>0$. 取 $c=\langle v_1, v_1\rangle^{-\frac{1}{2}}$并用 $w_1=cv_1$ 来代替 v_1.

接下来，我们找一个 w_1 和 v_2 的线性组合，使之与 w_1 正交. 这个线性组合就是 $w=v_2-aw_1$，其中 $a=\langle v_2, w_1\rangle$：$\langle w, w_1\rangle=\langle v_2, w_1\rangle-a\langle w_1, w_1\rangle=\langle v_2, w_1\rangle-a=0$. 将向量正规化为长度 1 得到向量 w_2，我们用它来代替 v_2. 对于型为点积的情形这一作用的几何解释见下面图示. 向量 aw_1 是 v_2 在 w_1 张成的子空间(直线上)上的正交投影.



241

这里是一般的做法. 设 $k-1$ 个向量 $w_1, \cdots, w_{k-1}$是标准正交的，并且$(w_1, \cdots, w_{k-1}, v_k, \cdots, v_n)$是一个基，我们如下调整 v_k：令 $a_i=\langle v_k, w_i\rangle$且

【1.24】
$$w = v_k - a_1w_1 - a_2w_2 - \cdots - a_{k-1}w_{k-1}.$$

则对 $i=1, \cdots, k-1$，w 与 w_i 正交，因为

$$\langle w, w_i\rangle = \langle v_k, w_i\rangle - a_1\langle w_1, w_i\rangle - a_2\langle w_2, w_i\rangle - \cdots - a_{k-1}\langle w_{k-1}, w_i\rangle.$$

而由于 $w_1, \cdots, w_{k-1}$标准正交，除了项$\langle w_i, w_i\rangle$为 1 外，其余所有项$\langle w_j, w_i\rangle(1\leqslant j\leqslant k-1)$都为零，因而上面的和成为

$$\langle w, w_i\rangle = \langle v_k, w_i\rangle - a_i\langle w_i, w_i\rangle = \langle v_k, w_i\rangle - a_i = 0.$$

将 w 的长度正规化为 1，得到向量 w_k，像前面一样用它替代 v_k. 则$(w_1, \cdots, w_k)$是标准正交的. 因为 v_k 属于$(w_1, \cdots, w_k; v_{k+1}, \cdots, v_n)$的张成，这个集合是一个基. 对 k 作归纳即可得到标准正交基的存在性. ■

定理(1.19)证明的最后一部分　由定理(1.22)得到定理(1.19)中(iii)蕴涵(i)这一事实. 因为如果 A 是对称的和正定的，则它在$\mathbb{R}^n$上定义的型$\langle X, Y\rangle=X^tAY$也是对称的和正定的. 这时，定理(1.22)告诉我们存在一个关于型$\langle X, Y\rangle=X^tAY$的$\mathbb{R}^n$的标准正交基 $\mathbf{B}'$. (这个基关于$\mathbb{R}^n$上通常的点积可能不是标准正交的.)另一方面，型$\langle X, Y\rangle$关于这个新基 $\mathbf{B}'$的矩阵 A'满足关系 $P^tA'P=A$(1.12)，而因为 $\mathbf{B}'$标准正交，所以 $A'=I$. 这样 $A=P^tP$. 这证明了(ii)，并且由于已经知道(i)与(ii)等价，这亦证明了(i). ■

遗憾的是，没有一个真正简单的方法可以确定一个矩阵是否是正定的. 最方便的判别法之一如下：用 A_i 表示矩阵 A 的左上角 $i\times i$ 子矩阵. 这样

$$A_1 = [a_{11}], \quad A_2 = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \quad A_3 = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}, \cdots, \quad A_n = A.$$

【1.25】定理 实对称 $n\times n$ 矩阵 A 是正定的当且仅当对每个 $i=1, 2, \cdots, n$，行列式 $\det A_i$ 为正.

例如，2×2 矩阵

【1.26】
$$A = \begin{bmatrix} a & b \\ b & d \end{bmatrix}$$

是正定的当且仅当 $a>0$ 且 $ad-bc>0$. 应用这一判别法，我们立即可以验证(1.15)的矩阵 A' 是正定的，这与它代表点积这一事实是一致的.

定理(1.25)的证明放在下一节的末尾.

第二节 对称型：正交性

本节我们考虑具有一个给定的对称双线性型$\langle ,\rangle$上的有限维实向量空间 V，但去掉上节所作的型是正定的假设. 使得$\langle v, v\rangle$的正值和负值都可取到的型称为是不定的. 物理学中的洛伦兹型

$$X^t AY = x_1 y_1 + x_2 y_2 + x_3 y_3 - c^2 x_4 y_4$$

是"时空"$\mathbb{R}^4$中的不定型的典型代表. 代表光速的系数 c 可被正规化为 1，于是关于某个给定的基，这个型的矩阵成为

【2.1】
$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}.$$

现在我们考虑刻画有限维实向量空间上的所有对称型的问题. 用于研究这样的型的基本概念仍是正交性. 但如果一个型不是正定的，则可能出现一个非零向量 v 自正交的情形：$\langle v, v\rangle=0$. 例如，当型由(2.1)定义时，对于向量$(1, 0, 0, 1)^t\in\mathbb{R}^4$就会出现这样的情形. 因而必须修正我们的几何直感. 结果表明这样的忧虑是不必要的. 我们有足够多非自正交的向量.

【2.2】命题 假设对称型$\langle ,\rangle$不恒为零. 则存在一个非自正交的向量 $v\in V$：$\langle v, v\rangle\neq 0$.

证明 型$\langle ,\rangle$不恒为零意味着存在一对向量 $v, w\in V$ 使得$\langle v, w\rangle\neq 0$. 取这两个向量，如果$\langle v, v\rangle\neq 0$，或$\langle w, w\rangle\neq 0$，则命题已得证. 假设$\langle v, v\rangle=\langle w, w\rangle=0$. 令 $u=v+w$，利用双线性展开$\langle u, u\rangle$：

$$\langle u,u\rangle = \langle v+w,v+w\rangle = \langle v,v\rangle + \langle v,w\rangle + \langle w,v\rangle + \langle w,w\rangle = 0 + 2\langle v,w\rangle + 0.$$

因为$\langle v, w\rangle\neq 0$，于是得到$\langle u, u\rangle\neq 0$. ■

如果 W 是 V 的子空间，则用 $W^\perp$ 表示与每一个 $w\in W$ 正交的全体向量 v 的集合：

【2.3】
$$W^\perp = \{v \in V \mid \langle v,W\rangle = 0\}.$$

这是 V 的子空间，称为 W 的正交补.

【2.4】命题 设 $w\in V$ 是一个使得$\langle w, w\rangle\neq 0$ 的向量. 令 $W=\{cw\}$是 w 的张成. 则 V 是 W 与

242

其正交补的直和：

243

$$V = W \oplus W^{\perp}.$$

证明 根据第三章(6.4)和(6.5)，我们要证两个结论：

(a) $W \cap W^{\perp} = 0$. 这是显然的. 因为$\langle cw, w\rangle = c\langle w, w\rangle$且$\langle w, w\rangle \neq 0$，所以除非$c=0$，否则向量$cw$不与$w$正交.

(b) W和$W^{\perp}$张成V：每一向量$v \in V$可以写为$v = aw + v'$的形式，其中$v' \in W^{\perp}$. 为证明这一点，我们关于a解方程$\langle v - aw, w\rangle = 0$：$\langle v-aw, w\rangle = \langle v, w\rangle - a\langle w, w\rangle = 0$. 其解为$a = \dfrac{\langle v, w\rangle}{\langle w, w\rangle}$. 这时取$v' = v - aw$即可. ■

还需要另外两个概念，它们是对称型的迷向空间和非退化型. 向量$v \in V$称为给定型的一个迷向向量，如果对所有$w \in V$有$\langle v, w\rangle = 0$，即如果v与整个空间V正交. 型的迷向空间是所有迷向向量的集合

【2.5】

$$N = \{v \mid \langle v, V\rangle = 0\} = V^{\perp}.$$

一个对称型称为非退化的，如果其迷向空间为$\{0\}$.

【2.6】命题 设A是对称型关于一个基的矩阵.

(a) 型的迷向空间是所有这样的向量v的集合：v的坐标向量X是齐次方程组$AX=0$的解.

(b) 型非退化当且仅当矩阵A非奇异.

证明 通过这个基，将型对应于积X^tAY[见(1.11)]. 我们对这个积来证明. 如果Y是满足$AY=0$的向量，则对所有X有$X^tAY=0$；因而Y属于迷向空间. 反之，假设$AY \neq 0$. 则AY至少有一个非零坐标. AY的第i个坐标是e_i^tAY. 因此这些积e_i^tAY中有一个非零. 这说明Y不是迷向向量，这就证明了(a). (b)由(a)得到. ■

下面是(2.4)的一个推广的版本：

【2.7】命题 设W是V的一个子空间，考虑对称型$\langle , \rangle$在W的限制. 如果这个型在W上非退化，则$V = W \oplus W^{\perp}$.

我们略去证明，它完全由(2.4)得到.

【2.8】定义 关于对称型$\langle , \rangle$的一个正交基$\mathbf{B} = (v_1, \cdots, v_n)$是使得对所有$i \neq j$都有$v_i \perp v_j$的基.

因为型的矩阵A由$a_{ij} = \langle v_i, v_j\rangle$定义，基$\mathbf{B}$是正交的当且仅当$A$是对角矩阵. 注意如果对称型$\langle , \rangle$是非退化的，且如果基$\mathbf{B} = (v_1, \cdots, v_n)$正交，则对所有$i$，有$\langle v_i, v_i\rangle \neq 0$：$A$的对角线上的元素都不为零.

244

【2.9】定理 设$\langle , \rangle$为实向量空间V的一个对称型.

(a) 存在V的一个正交基. 更精确地说，存在基$\mathbf{B} = (v_1, \cdots, v_n)$使得当$i \neq j$时$\langle v_i, v_j\rangle = 0$，而对每一$i$，$\langle v_i, v_i\rangle = 1$，$-1$或$0$.

(b) 矩阵形式：设A是实对称$n \times n$矩阵. 存在一个矩阵$Q \in GL_n(\mathbb{R})$使得QAQ^t是对角元素为1，-1或0的对角矩阵.

考虑到任意对称矩阵都是某个对称型的矩阵，(b)可由(a)及(1.13)得到.

可以置换正交基$\mathbf{B}$使得满足$\langle v_i, v_i\rangle = 1$的指标在前面，等等. 则矩阵$A$的形式成为

【2.10】
$$A=\begin{bmatrix} I_p & & \\ & -I_m & \\ & & 0_z \end{bmatrix},$$
其中 p 是 $+1$ 的个数，m 是 -1 的个数，z 是 0 的个数，因而 $p+m+z=n$. 这些数字由型或矩阵 A 唯一确定：

【2.11】定理 西尔维斯特法则：(2.10)中出现的数 p，m，z 是由型唯一确定的. 换言之，它们与使 $\langle v_i, v_i\rangle=\pm1$ 或 0 的正交基 $\boldsymbol{B}$ 的选择无关.

整数对(p, m)称为型的**符号差**.

定理(2.9)的证明 如果型恒等于 0，则关于任意基计算的矩阵 A 都是零矩阵，这是对角矩阵. 假设型不恒为零. 则由命题(2.2)，存在一个向量 $v=v_1$ 使得 $\langle v_1, v_1\rangle\neq0$. 设 W 是 v_1 的张成. 由命题(2.4)，$V=W\oplus W^{\perp}$，因而 V 的一个基由 W 的基(v_1)和 $W^{\perp}$ 的任意一个基$(v_2, \cdots, v_n)$组合得到[第三章(6.6)]. V 上的型可限制在子空间 $W^{\perp}$，它在其上定义一个型. 我们对维数用归纳得到 $W^{\perp}$ 有一个正交基$(v_2, \cdots, v_n)$. 则$(v_1, v_2, \cdots, v_n)$是 V 的一个正交基. 这是因为如果 $i>1$，则由于 $v_i\in W^{\perp}$，故有$\langle v_1, v_i\rangle=0$，且因为$(v_2, \cdots, v_n)$是正交基，如果$i, j>1$ 且 $i\neq j$，则$\langle v_i, v_j\rangle=0$.

还需要正规化刚构造出的正交基. 如果$\langle v_i, v_i\rangle\neq0$，我们解出 $c^{-2}=\pm\langle v_i, v_i\rangle$并将基向量 v_i 换成 cv_i. 则$\langle v_i, v_i\rangle$变为±1. 这就完成了(2.9)的证明. ■

245

定理(2.11)的证明 设 $r=p+m$.（这是矩阵 A 的秩.）设$(v_1, \cdots, v_n)$是 V 的具有所考虑的类型的正交基，也就是说，它使得矩阵为(2.10). 我们首先通过证明向量 $v_{r+1}, \cdots, v_n$ 构成迷向空间 $N=V^{\perp}$ 的基而证明数 z 是确定的. 这表明 $z=\dim N$，因此 z 与基的选择无关.

向量 $w\in V$ 是迷向向量当且仅当它与我们基中的每一个向量 v_i 正交. 将这个向量写成基的线性组合：$w=c_1v_1+\cdots+c_nv_n$. 则由于 $i\neq j$ 时$\langle v_i, v_j\rangle=0$，我们得到$\langle w, v_i\rangle=c_i\langle v_i, v_i\rangle$. 现在$\langle v_i, v_i\rangle=0$ 当且仅当 $i>r$. 因而要使 w 与每个 v_i 正交，则对所有 $i\leqslant r$ 必须有 $c_i=0$. 这表明$(v_{r+1}, \cdots, v_n)$张成 N，且作为线性无关的集合，它是 N 的基.

等式 $p+m+z=n$ 表明 $p+m$ 也已确定. 我们还需要证明剩下的两个整数 p，m 之一是也是确定的. 这点不是那么简单. 例如$(v_1, \cdots, v_p)$的张成由型唯一确定的说法是不对的.

假设给定第二个这样的基$(v_1', \cdots, v_n')$且得到整数 p'，m'(及 $z'=z$). 我们将证明 $p+(n-p')$个向量

【2.12】
$$v_1,\cdots,v_p;v'_{p'+1},\cdots,v'_n$$
是线性无关的. 于是由于 V 的维数为 n，得到 $p+(n-p')\leqslant n$，因此 $p\leqslant p'$，交换 p 与 p'的角色，得 $p=p'$.

设给定(2.12)向量间的一个线性关系. 可将其写为下面的形式：

【2.13】
$$b_1v_1+\cdots+b_pv_p=c_{p'+1}v'_{p'+1}+\cdots+c_nv'_n.$$
用 v 表示这两个表达式中任一个定义的向量. 我们用两种方式计算$\langle v, v\rangle$. 左边给出
$$\langle v,v\rangle=b_1^2\langle v_1,v_1\rangle+\cdots+b_p^2\langle v_p,v_p\rangle=b_1^2+\cdots+b_p^2\geqslant0,$$
而右边给出

$$\langle v,v\rangle = c_{p'+1}^2\langle v_{p'+1},v_{p'+1}\rangle + \cdots + c_n^2\langle v_n',v_n'\rangle = -c_{p'+1}^2 - \cdots - c_{p'+m'}^2 \leqslant 0.$$

由此得到 $b_1^2+\cdots+b_p^2=0$，因而 $b_1=\cdots=b_p=0$. 知道这一点，$(v_1', \cdots, v_n')$是基这个事实与(2.13)一起推出$c_{p'+1}=\cdots=c_n=0$. 因而，正是我们所要证明的，关系是平凡的. ■

为了讨论不定型，常用记号 $I_{p,m}$表示对角矩阵

【2.14】
$$I_{p,m}=\begin{bmatrix} I_p & \\ & -I_m \end{bmatrix}.$$

用这个记号，代表洛伦兹型(2.1)的矩阵是 $I_{3,1}$.

246

我们现在证明定理(1.25)——矩阵 A 是正定的当且仅当对所有 i 有 $A_i>0$.

定理(1.25)的证明 假设型 X^tAY是正定的. $\mathbb{R}^n$的基变换把矩阵变为$A'=QAQ^t$，且

$$\det A' = (\det Q)(\det A)(\det Q^t) = (\det Q)^2(\det A).$$

由于它们差一个平方因子，因此 $\det A'$为正当且仅当 $\det A$ 为正. 由(1.19)，可选一个矩阵 Q 使得 $A'=I$，因为 I 有行列式 1，故 $\det A>0$.

矩阵 A_i 表示型在由$(v_1, \cdots, v_i)$张成的子空间上的限制，当然，型在 V_i 上是正定的. 因此，和 $\det A>0$ 同样的理由，$\det A_i>0$.

反之，假设对所有 i，$\det A_i$ 为正. 对 n 作归纳，可假设型在 V_{n-1}上正定. 因而存在矩阵 $Q'\in GL_{n-1}$使得 $Q'A_{n-1}Q'^t=I_{n-1}$. 设 Q 为矩阵

$$\begin{bmatrix} Q' & \\ & 1 \end{bmatrix}.$$

则

$$QAQ^t=\begin{bmatrix} & & * \\ & I & \vdots \\ * & \cdots & * \end{bmatrix}.$$

我们现在用初等行变换 $E_1, \cdots, E_{n-1}$消去除(n, n)元外的最后一行. 令 $P=E_{n-1}\cdots E_1Q$. 则

$$A'=PAP^t=\begin{bmatrix} \begin{bmatrix} & & \\ & I & \\ & & \end{bmatrix} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \begin{matrix} 0 & \cdots & 0 \end{matrix} & c \end{bmatrix}$$

对某个 c 成立. 因为 $A'=PAP^t$ 是对称的，最后一列也被消去. 由于 $\det A>0$，我们也有 $\det A'=(\det A)(\det P)^2>0$，这蕴涵 $c>0$. 因此矩阵 A'代表正定型. 它与 A 代表同一个型. 因而 A 是正定的.

第三节　正定型相关的几何

本节我们再次转到对 n-维实向量空间 V 上的一个正定双线性型$\langle,\rangle$的研究. 具有一个这样的型的实向量空间称为一个欧几里得空间.

类似于$\mathbb{R}^n$中向量的长度[第四章(5.10)]的定义，自然地可用法则

【3.1】
$$|v|=\sqrt{\langle v, v\rangle}$$

定义向量 v 的长度. 型为正定的这个事实的一个重要的结果是可以通过计算其长度来确定一个向量 v 是否为零： 247

【3.2】
$$v = 0 \quad 当且仅当 \quad \langle v,v\rangle = 0.$$

正如我们在第一节所指出的，V 中存在一个标准正交基 $\boldsymbol{B}=(v_1, \cdots, v_n)$，因而这个型对应于$\mathbb{R}^n$的点积：如果 $v=\boldsymbol{B}X$ 而 $w=\boldsymbol{B}Y$，则

$$\langle v,w\rangle = X^tY.$$

利用这一对应，可将$\mathbb{R}^n$的几何转移到 V 上. 每当我们在欧氏空间 V 中遇到问题，自然的办法是选择方便的标准正交基，从而将问题归结到$\mathbb{R}^n$的点积这一熟悉的情形.

当给定 V 的一个子空间 W，我们有两件事可做. 第一件事是把型$\langle ,\rangle$限制到子空间，即简单地把型在 W 中一对向量 w_1，w_2 上的值定义为$\langle w_1, w_2\rangle$. 双线性型在子空间 W 上的限制是 W 上的双线性型，如果这个型是对称的或者如果它是对称的和正定的，则其限制也是.

型的限制可用于定义两个向量 v，w 间的无向夹角. 如果这两个向量线性相关，其夹角为零. 否则，(v, w)是 V 的一个二维子空间 W 的基. 型在 W 上的限制仍是正定的，因而存在 W 的标准正交基(w_1, w_2). 通过这个基，v，w 对应于它们在$\mathbb{R}^2$中的坐标向量 X，Y. 这使我们能通过 X，Y 的性质解释向量 v，w 的几何性质.

由于基(w_1, w_2)是标准正交的，型对应于$\mathbb{R}^2$的点积：$\langle v, w\rangle=X^tY$. 因此

$$|v|=|X|, \quad |w|=|Y|, \quad \langle v,w\rangle = (X\cdot Y).$$

我们定义 v，w 间的夹角 θ 为 X 与 Y 间的夹角，由此，作为$\mathbb{R}^2$中点积的类似的公式[第四章(5.11)]的结果，得到公式

【3.3】
$$\langle v,w\rangle = |v||w|\cos\theta.$$

这个公式中用其他几个符号确定了 $\cos\theta$，除了± 1 因子外 $\cos\theta$ 确定 θ. 因而 v 与 w 间的夹角在相差一个符号下由型本身确定. 这是我们所能得到的最好的结果，即使在$\mathbb{R}^3$也只能是这样.

像施瓦兹不等式

【3.4】
$$|\langle v,w\rangle| \leqslant |v||w|$$

和三角不等式

【3.5】
$$|v+w| \leqslant |v|+|w|$$

等标准事实都可以通过限制到二维子空间的任意的欧几里得空间加以证明. 248

当给定子空间 W 以后，我们可以做的第二件事是将 V 投射到 W. 因为型在 W 的限制是正定的，所以它是非退化的. 因而由(2.17)，$V=W\oplus W^{\perp}$，所以每个 $v\in V$ 有唯一的表达式

【3.6】
$$v = w + w', \quad 其中\ w \in W \quad 且 \quad \langle w,w'\rangle = 0.$$

正交投影 π：$V \longrightarrow W$ 定义为线性变换

【3.7】
$$v \rightsquigarrow \pi(v) = w,$$

其中 w 由(3.6)给出.

用 W 的标准正交基$(w_1, \cdots, w_r)$可以很容易算出投影向量 $\pi(v)$. 下面是一个重要结果：

【3.8】命题 设$(w_1, \cdots, w_r)$是子空间 W 的一个标准正交基，并设 $v\in V$. 则 v 到 W 的正交投影 $\pi(v)$是向量

$$\pi(v) = \langle v,w_1\rangle w_1 + \cdots + \langle v,w_r\rangle w_r.$$

这样，如果π由上面的公式定义，则$v-\pi(v)$与W正交．这一公式解释了第一节描述的格拉姆-施密特过程的几何意义．

证明 用$\tilde{w}$表示上述等式的右边．则$\langle \tilde{w}, w_i\rangle = \langle v, w_i\rangle\langle w_i, w_i\rangle = \langle v, w_i\rangle$对$i=1, \cdots, r$成立，因此$v-\tilde{w}\in W^{\perp}$．由于$v$的表达式(3.6)是唯一的，故$w=\tilde{w}$且$w'=v-\tilde{w}$． ■

$W=V$时也很重要．这时π是恒等映射．

【3.9】推论 设$\boldsymbol{B}=(v_1, \cdots, v_n)$是欧几里得空间$V$的一个标准正交基．则

$$v = \langle v,v_1\rangle v_1 + \cdots + \langle v,v_n\rangle v_n.$$

换言之，v关于标准正交基$\boldsymbol{B}$的坐标向量是

$$X = (\langle v,v_1\rangle, \cdots, \langle v,v_n\rangle)^t.$$

第四节 埃尔米特型

本节我们假定标量域是复数域$\mathbb{C}$．当处理复向量空间时，希望有与向量长度类似的概念，当然可以将$\mathbb{C}^n$上的长度等同于$\mathbb{R}^{2n}$中而加以定义．如果$X=(x_1, \cdots, x_n)^t$是个复向量且如果$x_r=a_r+b_r\mathrm{i}$,则X的长度是

【4.1】 $$|X| = \sqrt{a_1^2+b_1^2+\cdots+a_n^2+b_n^2} = \sqrt{\bar{x}_1x_1+\cdots+\bar{x}_nx_n},$$

249 其中上划线表示复共轭．这个公式表明对于复向量作点积是“不合适的”，而应该用公式

【4.2】 $$\langle X,Y\rangle = \overline{X}^tY = \bar{x}_1y_1+\cdots+\bar{x}_ny_n$$

来定义一个积．这个积具有正性：

【4.3】 如果$X\neq 0$，则$\langle X, X\rangle$是正实数．

此外，(4.2)与实向量的点积一致．

积(4.2)称为标准埃尔米特积，或埃尔米特点积．它具有下述性质：

【4.4】

关于第二个变量线性：

$$\langle X,cY\rangle = c\langle X,Y\rangle \quad 且 \quad \langle X,Y_1+Y_2\rangle = \langle X,Y_1\rangle + \langle X,Y_2\rangle;$$

关于第一个变量共轭线性：

$$\langle cX,Y\rangle = \bar{c}\langle X,Y\rangle \quad 且 \quad \langle X_1+Y_2,Y\rangle = \langle X_1,Y\rangle + \langle X_2,Y\rangle;$$

埃尔米特对称：

$$\langle Y,X\rangle = \overline{\langle X,Y\rangle}.$$

这样我们可以用线性和对称性方面很小的代价得到了一个正定积．

当需要用到涉及长度的概念时，埃尔米特积是正确的选择，虽然在应用中复向量空间上对称双线性型也会出现．

若V是复向量空间，V上的一个埃尔米特型是任一满足条件(4.4)的两个变量的函数

【4.5】 $$V\times V \longrightarrow \mathbb{C}$$
$$v,w \rightsquigarrow \langle v,w\rangle.$$

设 $\mathbf{B}=(v_1, \cdots, v_n)$ 是 V 的一个基. 则型的矩阵用类似于双线性型的矩阵的方式定义：

$$A=(a_{ij}), \quad \text{其中} \quad a_{ij}=\langle v_i, v_j\rangle.$$

型的公式现在成为

【4.6】

$$\langle v, w\rangle=\overline{X}^{\mathrm{t}} A Y,$$

其中 $v=\mathbf{B}X$ 而 $w=\mathbf{B}Y$.

矩阵 A 不是任意的，因为埃尔米特对称蕴涵

$$a_{ij}=\langle v_i, v_j\rangle=\overline{\langle v_j, v_i\rangle}=\bar{a}_{ji},$$

即 $A=\overline{A}^{\mathrm{t}}$. 我们引入矩阵 A 的伴随[与第一章(5.4)所定义的那个不同]为

250

【4.7】

$$A^*=\overline{A}^{\mathrm{t}}.$$

它满足如下规则：

$$(A+B)^*=A^*+B^*$$

$$(AB)^*=B^*A^*$$

$$(A^*)^{-1}=(A^{-1})^*$$

$$A^{**}=A.$$

这些规则是容易验证的. 公式(4.6)现在可以重新写作

【4.8】

$$\langle v, w\rangle=X^* A Y,$$

而且 $\mathbb{C}^n$ 上的标准埃尔米特型成为 $\langle X, Y\rangle=X^*Y$.

一个矩阵 A 称为埃尔米特的或者自伴随的，如果

【4.9】

$$A=A^*,$$

埃尔米特矩阵正好是埃尔米特型的矩阵. 其元素满足条件 $a_{ji}=\bar{a}_{ij}$. 这蕴涵对角元素是实的并且对角线下的元素是对角线上的元素的复共轭：

$$A=\begin{bmatrix} r_1 & & a_{ij} \\ & \ddots & \\ \bar{a}_{ij} & & r_n \end{bmatrix}, \quad r_i \in \mathbb{R}, \quad a_{ij} \in \mathbb{C}.$$

例如，$\begin{bmatrix} 2 & \mathrm{i} \\ -\mathrm{i} & 1 \end{bmatrix}$ 是一个埃尔米特矩阵.

注意实矩阵是埃尔米特矩阵的条件是 $a_{ji}=a_{ij}$：

【4.10】 实埃尔米特矩阵是实对称矩阵.

第一节和第二节对基变换的讨论对于埃尔米特型有类似的结果. 给一个定埃尔米特型，由矩阵 P 产生的基变换如(1.12)一样给出

$$X'^* A' Y'=(PX)^* A' PY=X^*(P^* A' P) Y.$$

因此新矩阵 A' 满足条件

【4.11】

$$A=P^* A' P, \quad \text{或} \quad A'=(P^*)^{-1} A P^{-1}.$$

由于 P 是任意的，可用 $Q=(P^*)^{-1}$ 代替它而得到类似于(1.13)的刻画：

【4.12】推论 设 A 是一个埃尔米特型关于一个基的矩阵. 在不同的基下代表同一个埃尔米特型的矩阵具有 $A'=QAQ^*$ 的形式，其中 $Q \in GL_n(\mathbb{C})$ 是一个可逆矩阵.

251

对于埃尔米特型，类似于正交矩阵的是酉矩阵．矩阵 P 称为酉的，如果它满足条件

【4.13】 $$P^*P=I \quad 或 \quad P^*=P^{-1}.$$

例如，$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & \mathrm{i}\\ 1 & -\mathrm{i}\end{bmatrix}$是一个酉矩阵．

注意对于实矩阵 P，这个条件变为 $P^tP=I$：

【4.14】实酉矩阵是实正交矩阵．

酉矩阵构成一个群，即酉群 U_n：

【4.15】 $$U_n=\{P \mid P^*P=I\}.$$

公式(4.11)告诉我们酉矩阵代表使标准埃尔米特积 X^*Y 不变的基变换：

【4.16】推论 一个基变换保持标准埃尔米特积，即 $X^*Y=X'^*Y'$，当且仅当其矩阵 P 是酉的．

但推论(4.12)告诉我们一般的基变换将标准埃尔米特积 X^*Y 变为 $X'^*A'Y'$，其中 $A'=QQ^*$，而 $Q\in GL_n(\mathbb{C})$．

对于埃尔米特型的正交概念的定义和对称双线性型是完全一样的：v 称为与 w 正交，如果 $\langle v, w\rangle=0$．由于$\overline{\langle v, w\rangle}=\langle w, v\rangle$，正交仍是一个对称关系．现在可将第一节和第二节的讨论复制到埃尔米特型而不必做本质上的改动，且实对称型的西尔维斯特法则也可搬到埃尔米特型上来．特别地，可以讨论正定型，也就是那些具有性质

【4.17】 $$如果\ v\neq 0，则\langle v, v\rangle 为正实数$$

的型和标准正交基 $\mathbf{B}=(v_1, \cdots, v_n)$，即满足

【4.18】 $$\langle v_i, v_i\rangle=1 \quad 且如果\ i\neq j，则\langle v_i, v_j\rangle=0$$

的基．

【4.19】定理 设$\langle\,,\rangle$是复向量空间 V 上的埃尔米特型．V 中存在标准正交基当且仅当型是正定的．

【4.20】命题 设 W 是埃尔米特空间 V 的子空间．若型在 W 的限制非退化，则 $V=W\oplus W^{\perp}$．

252 这些结论的证明留作练习．

第五节 谱 定 理

本节将研究 n-维复向量空间 V 和 V 上的正定埃尔米特型$\langle\,,\rangle$．具有正定埃尔米特型的复向量空间 V 称为埃尔米特空间．如果有必要的话，可把空间 V 想象为带有标准埃尔米特积 X^*Y 的空间$\mathbb{C}^n$．在 V 中选择一个标准正交基使我们能作出这样的等同．

由于型$\langle\,,\rangle$是给定的，我们不想在 V 中随便取一个基来计算．自然是只使用标准正交基．这使得前面的计算有了如下的改变：基变换矩阵 P 不再是任意的可逆矩阵．取而代之的是，如果 $\mathbf{B}=(v_1, \cdots, v_n)$，$\mathbf{B}'=(v_1', \cdots, v_n')$是两个标准正交基，则联系它们的矩阵 P 是酉的．基是标准正交的这一事实表明型$\langle\,,\rangle$关于每个基的矩阵是单位矩阵 I，于是(4.11)指出 $I=P^*IP$ 或$P^*P=I$．

我们将研究空间 V 上的线性算子

【5.1】 $$T: V\longrightarrow V.$$

设 $\mathbf{B}$ 是标准正交基，M 是 T 对应的矩阵．标准正交基的变换使 M 变为 $M'=PMP^{-1}$［第四章

(3.4)]，其中 P 是酉的；因而

【5.2】
$$M' = PMP^*.$$

【5.3】命题　设 T 是埃尔米特空间 V 上的线性算子，设 M 是 T 关于标准正交基 $\mathbf{B}$ 的矩阵.

(a) 矩阵 M 是埃尔米特的当且仅当对所有 $v, w \in V$，有 $\langle v, Tw\rangle = \langle Tv, w\rangle$. 这时，称 T 为埃尔米特算子.

(b) 矩阵 M 是酉的当且仅当对所有 $v, w \in V$，有 $\langle v, w\rangle = \langle Tv, Tw\rangle$. 这时，称 T 为酉算子.

证明　设 X, Y 是 v, w 的坐标向量：$v = \mathbf{B}X$，$w = \mathbf{B}Y$，从而 $\langle v, w\rangle = X^*Y$，$Tv = \mathbf{B}MX$. 于是 $\langle v, Tw\rangle = X^*MY$，而 $\langle Tv, w\rangle = X^*M^*Y$. 因而若 $M = M^*$，则对所有 $v, w \in V$，有 $\langle v, Tw\rangle = \langle Tv, w\rangle$；即 T 是埃尔米特的. 反之，如果 T 是埃尔米特的，如同在(1.9)的证明中一样，令 $v = e_i$，$w = e_j$，便得到 $b_{ij} = e_i^*(Me_j) = (e_i^*M^*)e_j = \bar{b}_{ji}$. 这样 $M = M^*$. 类似地，$\langle v, w\rangle = X^*Y$ 且 $\langle Tv, Tw\rangle = X^*M^*MY$，因而对所有 $v, w \in V$，$\langle v, w\rangle = \langle Tv, Tw\rangle$ 当且仅当 $M^*M = I$. ■

【5.4】定理　谱定理：

(a) 设 T 是埃尔米特空间 V 上的埃尔米特算子. 存在由 T 的特征向量组成的 V 的一个标准正交基.

(b) 矩阵形式：设 M 是埃尔米特矩阵. 存在酉矩阵 P 使得 PMP^* 为实对角矩阵.

253

证明　选择一个特征向量 $v = v_1$，正规化使之长度为 1：$\langle v, v\rangle = 1$. 扩张为一个标准正交基. 则 T 的矩阵变为

$$M = \begin{bmatrix} a & * & \cdots & * \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{bmatrix}.$$

由于 T 是埃尔米特的，矩阵 M 也是埃尔米特的(5.3). 由此得到 $*\cdots* = 0\cdots0$ 并且 N 是埃尔米特矩阵. 用归纳法继续即可. ■

通过确定特征向量可以用一个酉矩阵 P 来对角化一个埃尔米特矩阵 M. 如果特征值是互不相同的，则对应的特征向量是正交的. 这可由谱定理得到. 设 $\mathbf{B}'$ 是通过将特征向量的长度正规化到 1 而得到的标准正交基. 则 $P = [\mathbf{B}']^{-1}$[第三章(4.20)].

例如，设

$$M = \begin{bmatrix} 2 & i \\ -i & 2 \end{bmatrix}.$$

这个矩阵的特征值为 3，1，而向量

$$v_1' = \begin{bmatrix} 1 \\ -i \end{bmatrix}, \quad v_2' = \begin{bmatrix} 1 \\ i \end{bmatrix}$$

是有这两个特征值的特征向量. 用因子 $\frac{1}{\sqrt{2}}$ 将其长度正规化到 1. 则

$$P=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\-\mathrm{i}&\mathrm{i}\end{bmatrix}^*=\frac{1}{\sqrt{2}}\begin{bmatrix}1&\mathrm{i}\\1&-\mathrm{i}\end{bmatrix}\quad 及\quad PMP^*=\begin{bmatrix}3&\\&1\end{bmatrix}.$$

但谱定理断言即使其特征值不是不同的，埃尔米特矩阵也可以对角化．对于 2×2 矩阵叙述起来特别简单：如果 2×2 埃尔米特矩阵 M 的特征多项式有重根，则存在酉矩阵 P 使得 $PMP^*=aI$．将 P 移到方程的另一边，得到 $M=P^*aIP=aP^*P=aI$．因而由谱定理得到 $M=aI$．仅有的特征多项式有重根的 2×2 埃尔米特矩阵为矩阵 aI，其中 a 是实数．我们可以由定义直接验证这一事实．记 $M=\begin{bmatrix}a&\beta\\\bar{\beta}&d\end{bmatrix}$，其中 a，d 是实数而 β 为复数．则其特征多项式为 $t^2-(a+d)t+(ad-\beta\bar{\beta})$．这个多项式有重根当且仅当其判别式为零，即如果

254

$$(a+d)^2-4(ad-\beta\bar{\beta})=(a-d)^2+4\beta\bar{\beta}=0.$$

$(a-d)^2$ 和 $\beta\bar{\beta}$ 两项都是非负实数．因而如果判别式为零，则 $a=d$ 且 $\beta=0$．这时，正如我们所预测的，有 $M=aI$．

下面是谱定理的一个有趣的结果，我们可以给出它的一个直接证明．

【5.5】命题 埃尔米特算子的特征值是实数．

证明 设 a 是 T 的一个特征值，而 v 是一个特征向量，满足 $T(v)=av$．则由(5.3)，$\langle Tv,v\rangle=\langle v,Tv\rangle$；因此 $\langle av,v\rangle=\langle v,av\rangle$．由共轭线性(4.4)，

$$\bar{a}\langle v,v\rangle=\langle av,v\rangle=\langle v,av\rangle=a\langle v,v\rangle,$$

且由于型 $\langle\,,\rangle$ 正定，$\langle v,v\rangle\neq0$．因此 $a=\bar{a}$．这表明 a 是实的． ■

我们对埃尔米特矩阵所证明的结果对于实对称矩阵有类似的结果．设 V 是具有正定双线性型 $\langle\,,\rangle$ 的实向量空间．设 T 是 V 的一个线性算子．

【5.6】命题 设 M 是 T 的关于一个标准正交基的矩阵．

(a) 矩阵 M 是对称的当且仅当对所有 v，$w\in V$，有 $\langle v,Tw\rangle=\langle Tv,w\rangle$．这时称 T 为一个对称算子．

(b) 矩阵 M 是正交的当且仅当对所有 v，$w\in V$，有 $\langle v,w\rangle=\langle Tv,Tw\rangle$．这时称 T 为一个正交算子．

【5.7】命题 实对称矩阵的特征值是实的．

证明 实对称矩阵是埃尔米特的．因而这是(5.5)的特殊情形． ■

【5.8】定理 谱定理(实情形)：

(a) 设 T 是具有正定双线性型的一个实向量空间 V 上的对称算子．存在一个由 T 的特征向量组成的标准正交基．

(b) 矩阵形式：设 M 是实对称 $n\times n$ 矩阵．存在正交矩阵 $P\in O_n(\mathbb{R})$ 使得 PMP^t 为实对角矩阵．

证明 我们知道这样一个算子的特征值是实的，只要复制(5.4)的证明即可． ■

第六节 圆锥曲线与二次曲面

圆锥曲线是由形如

255

【6.1】 $$f(x_1,x_2)=a_{11}x_1^2+2a_{12}x_1x_2+a_{22}x_2^2+b_1x_1+b_2x_2+c=0$$

的两个变量的二次方程所定义的平面$\mathbb{R}^2$ 中的轨迹. 更精确地说，轨迹(6.1)是圆锥曲线，意味着它是椭圆、双曲线或抛物线，不然的话就称为**退化的**. 退化的圆锥曲线按照其方程不同，可以是一对直线、单独一条直线、一个点或空集. **二次曲面**这一术语用于表示三维或更高维空间中类似的轨迹.

$f(x_1, x_2)$的二次部分称为**二次型**：

【6.2】

$$q(x_1,x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2.$$

一般来说，n 个变量 x_1，…，x_n 的二次型是其每一项关于变量的次数为 2 的多项式.

用矩阵记号表达型 $q(x_1, x_2)$会很方便. 为此，我们引入对称矩阵

【6.3】

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{bmatrix}.$$

于是 $q(x_1, x_2)=X^tAX$，其中 X 表示列向量$(x_1, x_2)^t$. 我们还引入行向量 $B=(b_1, b_2)$. 则方程(6.1)可以用矩阵记号写成

【6.4】

$$X^tAX + BX + c = 0.$$

在公式(6.1)和(6.2)中加上系数 2 以避免在矩阵(6.3)中一些系数为$\frac{1}{2}$. 二次型的另一个记法是

$$q(x_1,x_2) = a_{11}x_1^2 + a_{12}x_1x_2 + a_{12}x_2x_1 + a_{22}x_2^2.$$

我们要刻画圆锥曲线作为几何图形的全等类，也就是刻画它们在平面刚体运动作用下的轨道. 一个刚体运动将在方程(6.1)中产生一个变量代换.

【6.5】定理 每一个非退化的圆锥曲线与下列之一全等：

(i) 椭圆： $a_{11}x_1^2+a_{22}x_2^2-1=0$,

(ii) 双曲线： $a_{11}x_1^2-a_{22}x_2^2-1=0$,

(iii) 抛物线： $a_{11}x_1^2-x_2=0$， 其中 a_{11}，$a_{22}>0$.

证明 我们分两步化简方程(6.1)，首先应用正交算子(旋转或反射)对角化 A，然后应用平移，尽可能多地消去线性和常数项 $BX+c$.

由谱定理(5.8)，存在正交矩阵 P 使得 PAP^t 是对角矩阵. 作变量代换 $X'=PX$ 或 $X=P^tX'$. 代入方程(6.4)得

【6.6】

$$X'^t(PAP^t)X' + (BP^t)X' + c = 0.$$

因此存在变量的正交变换使二次型成为对角的，也就是使 x_1x_2 的系数 a_{12} 为零.

假设 A 是对角的. 则 f 形如

$$f(x_1,x_2) = a_{11}x_1^2 + a_{22}x_2^2 + b_1x_1 + b_2x_2 + c = 0.$$

通过配方消去 b_i，作代换

【6.7】

$$x_i = \left(x_i' - \frac{b_i}{2a_{ii}}\right).$$

代换的结果是

【6.8】

$$f(x_1,x_2) = a_{11}x_1'^2 + a_{22}x_2'^2 + c',$$

其中 c'根据需要可以是个确定的数. 这一代换对应于用向量$(b_1/2a_{11}, b_2/2a_{22})^t$ 作的平移，只要 a_{11}，a_{22}都不为零，我们就可做这个代换.

256

如果 $a_{ii}=0$ 而 $b_i\neq 0$，则可用代换

【6.9】
$$x_i = x_i' - \frac{c}{b_i}$$

消去常数项. 可将一个系数正规化到 -1. 这样做并去掉退化的圆锥曲线，剩下的是定理中的三种情形. 不难看出，除了在椭圆方程中交换 a_{11}，a_{22} 的情形以外，改变系数 a_{11}，a_{22} 将得到不同的全等类. ■

上面所用的方法可应用于任意多个变量从而对 n 维二次曲面进行分类. 一般二次方程形如

【6.10】
$$f(x_1,\cdots,x_n) = \sum_i a_{ii}x_i^2 + \sum_{i<j} 2a_{ij}x_ix_j + \sum_i b_ix_i + c = 0.$$

还可把方程更紧凑地写作

【6.11】
$$f(x_1,\cdots,x_n) = \sum_{i,j} a_{ij}x_ix_j + \sum_i b_ix_i + c = 0,$$

其中第一个和取遍所有的指标对，并且令 $a_{ji}=a_{ij}$.

我们定义矩阵 A，B 为

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{12} & & & \vdots \\ \vdots & & & \vdots \\ a_{1m} & & \cdots & a_{mm} \end{bmatrix},\quad B = (b_1,\cdots,b_n).$$

则二次型为

【6.12】
$$q(x_1,\cdots,x_n) = X^tAX,$$

和

257 【6.13】
$$f(x_1,\cdots,x_n) = X^tAX + BX + c.$$

通过适当的正交变换 P，二次曲面变成(6.6)，其中 PAP^t 是对角的. 当 A 是对角矩阵时，线性项由平移(6.7)或者使用(6.9)消去.

下面是三个变量曲面的分类：

【6.14】定理 $\mathbb{R}^3$ 中非退化的二次曲面的全等类由下列代表：

(i) 椭球面： $a_{11}x_1^2+a_{22}x_2^2+a_{33}x_3^2-1=0$,

(ii) 1-叶双曲面： $a_{11}x_1^2+a_{22}x_2^2-a_{33}x_3^2-1=0$,

(iii) 2-叶双曲面： $a_{11}x_1^2-a_{22}x_2^2-a_{33}x_3^2-1=0$,

(iv) 椭圆抛物面： $a_{11}x_1^2+a_{22}x_2^2-x_3=0$,

(v) 双曲抛物面： $a_{11}x_1^2-a_{22}x_2^2-x_3=0$,

其中 a_{11}，a_{22}，$a_{33}>0$.

给定二次方程 $f(x_1, x_2)=0$，通过使用非正交的坐标变换可以很容易地确定它所代表的圆锥曲线的美型. 例如，如果对应的二次型 q 是正定的，则圆锥曲线或是椭圆，或是退化的(单点或空集). 为区别这些情形，允许使用任意的坐标变换. 一个非正交坐标变换将使圆锥曲线变形，但不会把一个椭圆变为一个双曲线或一个退化的圆锥曲线.

作为例子，考虑轨迹

【6.15】
$$x_1^2+x_1x_2+x_2^2+4x_1+3x_2+4=0.$$
相应的矩阵为
$$A=\begin{bmatrix}1 & \frac{1}{2}\\ \frac{1}{2} & 1\end{bmatrix},$$
由(1.25)，它是正定的．我们用非正交变换 $X'=PX$ 对角化 A，其中
$$P=\begin{bmatrix}1 & \frac{1}{2}\\ & 1\end{bmatrix},\quad PAP^t=\begin{bmatrix}1 & \\ & \frac{3}{4}\end{bmatrix},\quad BP^t=(4,1),$$
这样得到
$$x_1'^2+\frac{3}{4}x_2'^2+4x_1'+x_2'+4=0.$$
配方后得到
$$x_1''^2+\frac{3}{4}x_2''^2-\frac{1}{3}=0,$$
它是个椭圆．这样(6.15)也代表一个椭圆．另一方面，如果把(6.15)的常数项换为5，则轨迹为空．

第七节　正规算子的谱定理

谱定理(5.4)告诉我们任意埃尔米特矩阵 M 可通过一个酉矩阵 P 变换为一个实对角矩阵 D：$D=PMP^*$．我们现在求矩阵 M，它可以用同样方式变化为一个对角矩阵 D，但这里不再要求 D 是实的．结果是这样的矩阵有一个非常优美的形式刻画．

【7.1】定义　矩阵 M 称为正规的，如果它与它的伴随交换，即 $MM^*=M^*M$.

【7.2】引理　若 M 是正规的且 P 是酉的，则 $M'=PMP^*$ 也是正规的，反之亦然．

证明　假设 M 是正规的．则 $M'M'^*=PMP^*(PMP^*)^*=PMM^*P^*=PM^*MP^*=(PMP^*)^*(PMP^*)=M'^*M'$．因而 PMP^* 正规．用 P^* 替代 P 就得到了其逆．■

这个引理使我们能在埃尔米特空间 V 上定义正规算子 $T: V\to V$ 为关于任意标准正交基的矩阵 M 都是正规矩阵的线性算子．

【7.3】定理　复矩阵 M 是正规的当且仅当存在酉矩阵 P 使得 PMP^* 为对角的．

除了埃尔米特矩阵外，最重要的正规矩阵是酉矩阵：因为如果 M 是酉的，则 $M^*=M^{-1}$，所以 $MM^*=M^*M=I$，这表明 M 是正规的．

【7.4】推论　酉群中每一共轭类含有一个对角矩阵．

定理(7.3)的证明　首先，任意两个对角矩阵可交换，因而对角矩阵是正规的：$DD^*=D^*D$．引理告诉我们，如果 $PMP^*=D$，则 M 是正规的．反过来，假设 M 正规，选择 M 的一个特征向量 $v=v_1$，像(5.4)的证明一样，作正规化使得 $\langle v, v\rangle=1$．将 $\{v_1\}$ 扩张成为一个标准正交基．则 M 变为矩阵

$$M_1 = PMP^* = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{bmatrix}, \quad M_1^* = PM^*P^* = \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ \bar{a}_{12} & & & \\ \vdots & & N^* & \\ \bar{a}_{1n} & & & \end{bmatrix}.$$

$M_1^* M_1$ 左上角的元素是 $a_{11}\bar{a}_{11}$，而 $M_1 M_1^*$ 中同样的元素是 $a_{11}\bar{a}_{11} + a_{12}\bar{a}_{12} + \cdots + a_{1n}\bar{a}_{1n}$. 由于 259 M 正规，因此 M_1 也正规，即 $M_1^* M_1 = M_1 M_1^*$. 从而得到 $a_{12}\bar{a}_{12} + \cdots + a_{1n}\bar{a}_{1n} = 0$. 由于 $a_{1j}\bar{a}_{1j} \geqslant 0$，这表明 $j > 1$ 时 a_{1j} 为 0，并且

$$M_1 = \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{bmatrix}.$$

对 N 继续即可. ■

第八节 斜对称型

258 斜对称型的理论与标量域无关. 有人会认为对于特征 2 的域会遇到麻烦，在这一情形中 $1+1=0$. 它们看起来是奇怪的，因为对所有 a 都有 $a=-a$，因而对称的条件(1.5)和斜对称的条件(1.6)是一样的. 如果改变斜对称的定义的话，结果是特征为 2 的域不会对斜对称型引起麻烦. 对所有域都适用的定义如下：

【8.1】定义 向量空间 V 上的双线性型 $\langle,\rangle$ 是斜对称的，如果

$$\langle v, v \rangle = 0$$

对所有 $v \in V$ 成立.

在这个定义下，对所有 $v, w \in V$，法则

【8.2】 $$\langle v, w \rangle = -\langle w, v \rangle$$

继续成立. 通过展开

$$\langle v+w, v+w \rangle = \langle v, v \rangle + \langle v, w \rangle + \langle w, v \rangle + \langle w, w \rangle,$$

并利用 $\langle v, v \rangle = \langle w, w \rangle = \langle v+w, v+w \rangle = 0$ 来证明它. 如果标量域的特征不是 2，则(8.1)和(8.2)是等价的. 因为如果(8.2)对所有 v, w 成立，则当令 $w=v$ 时，我们得 $\langle v, v \rangle = -\langle v, v \rangle$. 这蕴涵 $2\langle v, v \rangle = 0$，因而除非在标量域中 $2=0$，否则都有 $\langle v, v \rangle = 0$.

注意如果 F 的特征为 2，则在 F 中有 $1=-1$，故(8.2)表明型实际上是对称的. 但大多数对称型不满足(8.1).

关于任意基的斜对称型的矩阵 A 由性质

【8.3】 $$a_{ii} = 0 \quad 及如果 \quad i \neq j \quad 则 \quad a_{ij} = -a_{ji}$$

刻画. 我们把这个性质取作斜对称矩阵的定义. 如果特征不等于 2，这等价于条件

260 **【8.4】** $$A^t = -A.$$

【8.5】定理

(a) 设 V 是域 F 上的 m 维向量空间，并设 $\langle,\rangle$ 是 V 上非退化的斜对称型. 则 m 是偶数且存在 V 的基 $\boldsymbol{B}$ 使得型关于这个基的矩阵 A 是

$$J_{2n}=\begin{bmatrix}0 & I\\ -I & 0\end{bmatrix},$$

其中 $n=\frac{1}{2}m$，而 0，I 表示 $n\times n$ 矩阵.

(b) 矩阵形式：设 A 是非奇异斜对称 $m\times m$ 矩阵. 则 m 为偶数，并且存在矩阵 $Q\in GL_m(F)$ 使得 QAQ^t 为矩阵 J_{2n}.

如(8.6a)中，基 $\boldsymbol{B}$ 称为标准辛基. 注意按顺序(v_1，v_{n+1}，v_2，v_{n+2}，…，v_n，v_{2n})重新排列标准辛基将矩阵 J_{2n} 变为在对角线上由 2×2 的块

$$\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$$

构成的矩阵. 这是用来证明定理的最方便的形式. 我们将证明留作练习.

第九节　用矩阵记号对结果的小结

实数：一个方阵 A 是对称的，如果 $A^t=A$；A 是正交的，如果 $A^t=A^{-1}$.

(1) 谱定理：如果 A 是实对称矩阵，则存在正交矩阵 P 使得 $PAP^t(=PAP^{-1})$ 是对角的.

(2) 如果 A 是实对称矩阵，则存在一个实可逆矩阵 P 及整数 p，m，z 使得

$$PAP^t=\begin{bmatrix}I_p & & \\ & -I_m & \\ & & 0_z\end{bmatrix}.$$

(3) 西尔维斯特法则：数 p，m，z 由矩阵 A 确定.

复数：一个复方阵 A 是埃尔米特的，如果 $A^*=A$；A 是酉的，如果 $A^*=A^{-1}$；A 是正规的，如果 $AA^*=A^*A$.

(1)谱定理：如果 A 是埃尔米特矩阵，则存在酉矩阵 P 使得 PAP^* 是实对角矩阵.

(2)如果 A 是正规矩阵，则存在酉矩阵 P 使得 PAP^* 是对角的.

261

***F* 任意**：一个 $n\times n$ 方阵是斜对称的，如果 $a_{ii}=0$ 且对所有 i，j 有 $a_{ij}=-a_{ji}$. 如果 A 是可逆斜对称矩阵，则 n 是偶数，且存在一个可逆矩阵 P 使得 PAP^t 具有形式

$$\begin{bmatrix}0 & I\\ -I & 0\end{bmatrix}.$$

【9.1】注　由于坐标变换矩阵 P 定义的方式，双线性型的基变换法则(见(1.12)) $A'=(P^t)^{-1}A(P^{-1})$ 是相当难看的. 可以重新组织第三章的方程(4.7)，记

【9.2】
$$v_i'=\sum_j q_{ij}v_j \quad 或 \quad \boldsymbol{B}'^t=Q\boldsymbol{B}^t.$$

由此得 $Q=(P^{-1})^t$，用这个规则我们得到更好的公式

$$A'=QAQ^t,$$

以代替(1.12). 如果想要的话，可使用它.

公式(9.2)的问题是线性变换上的基变换乱成一团，即公式 $A'=PAP^{-1}$[第四章(3.4)]为 $A'=(Q^{-1})^{t}AQ^{t}$ 所替代. 保持公式简洁就像要保持一张毯子平整一样困难.

这带来了一个要点. 一旦一个基选定后，V 上的线性算子和 V 上的双线性型便各由一个 $n\times n$ 矩阵给出. 这会使人想到线性算子的理论和双线性型的理论在某种程度上是等价的，但除非基是固定的，否则它们是不等价的. 因为在基变换下双线性型的矩阵变为 $(P^{t})^{-1}AP^{-1}$，而线性算子的矩阵变为 PAP^{-1}[第四章(3.4)]. 因而新的矩阵不再相等. 更精确地讲，除非基变换的矩阵 P 碰巧是正交的，否则这只能表明当基改变后两个理论就分道扬飚了. 如果 P 正交，则$P=(P^{t})^{-1}$，这就好了，矩阵仍然相等. 这是使用标准正交基的一个好处.

Yvonne Verdier

练　习

第一节　双线性型的定义

262

1. 设 A 和 B 是实 $n\times n$ 矩阵. 证明如果对所有向量 $X, Y\in\mathbb{R}^n$ 有 $X^tAY=X^tBY$，则 $A=B$.
2. 直接证明由矩阵$\begin{bmatrix}a & b\\ b & d\end{bmatrix}$表示的双线性型是正定的当且仅当 $a>0$ 且 $ad-b^2>0$.
3. 当型为点积时，对基$(1, 1, 0)^t$，$(1, 0, 1)^t$，$(0, 1, 1)^t$ 应用格拉姆-施密特过程.
4. 设 $A=\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}$. 求$\mathbb{R}^2$关于型 X^tAY 的标准正交基.
5. (a) 证明每一个实方阵可以恰好用一种方式写为一个对称矩阵和一个斜对称矩阵($A^t=-A$)的和.
   (b) 设$\langle,\rangle$是实向量空间 V 的一个双线性型. 证明存在一个对称型$(,)$和一个斜对称型$[,]$使得$\langle,\rangle=(,)+[,]$.
6. 设$\langle,\rangle$是域 F 上向量空间 V 上的一个对称双线性型. 由 $q(v)=\langle v, v\rangle$定义的函数 q：$V\longrightarrow F$ 称为与双线性型相应的二次型. 如果域 F 的特征不是 2，说明如何通过展开 $q(v+w)$由 q 重新得出双线性型.
*7. 设 X，Y 是$\mathbb{C}^n$中的向量，并设 $X\neq 0$. 证明存在一个对称矩阵 B 使得 $BX=Y$.

第二节　对称型：正交性

1. 证明正定型是非退化的.
2. 一个矩阵 A 称为半正定的，如果对所有 $X\in\mathbb{R}^n$ 有 $X^tAX\geqslant 0$. 证明对任意 $m\times n$ 实矩阵 A，积 A^tA 是半正定的.
3. 求$\mathbb{R}^n$中其矩阵为如下所示的型的一个正交基.

   (a)$\begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}$　　(b)$\begin{bmatrix}1 & 0 & 1\\ 0 & 2 & 1\\ 1 & 1 & 1\end{bmatrix}$

4. 将向量 $X_1=(1, 1, 1)^t/\sqrt{3}$扩张为$\mathbb{R}^3$的一个标准正交基.
*5. 证明如果 $n\times n$ 矩阵 A 的列向量构成一个标准正交基，则行向量也构成一个标准正交基.
6. 设 A，A'为由 $A=P^tA'P$ 联系起来的对称矩阵，其中 $P\in GL_n(F)$. A 与 A'的秩相等对吗？
7. 设 A 为对称双线性型$\langle,\rangle$关于某个基的矩阵. 证明或推翻：A 的特征值与基无关.

8. 证明正交、对称、正定的实矩阵只有单位矩阵.
9. 次数$\leqslant n$的所有实多项式的向量空间P有由

$$\langle f,g\rangle=\int_{-1}^{1}f(x)g(x)\mathrm{d}x$$

定义的双线性型. 当n取值(a) 1, (b)2, (c) 3时, 求P的一个标准正交基.
10. 用V表示实$n\times n$矩阵的向量空间. 证明$\langle A, B\rangle=\mathrm{trace}(A^tB)$是$V$上的一个正定双线性型. 求这个型的一个标准正交基.

263

11. 一个对称矩阵A称为负定的, 如果对所有$X\neq 0$有$X^tAX<0$. 给出一个类似(1.26)的对称矩阵A为负定的判别法.
12. 证明每个对称非退化复矩阵具有$A=P^tP$的形式.
13. 用(2.12)的记号, 举例说明$(v_1, \cdots, v_t)$的张成不由型确定.
14. (a) 设W是有对称双线性型的向量空间V的子空间. 证明$W^\perp$是一个子空间.
    (b) 证明迷向空间N是个子空间.
15. 设W_1, W_2是有对称双线性型的向量空间V的子空间. 证明下列每一个关系成立.
    (a) $(W_1+W_2)^\perp=W_1^\perp\cap W_2^\perp$ (b) $W\subset W^{\perp\perp}$ (c) 如果$W_1\subset W_2$, 则$W_2^\perp\subset W_1^\perp$.
16. 证明命题(2.7), 即如果型在W上非退化, 则$V=W\oplus W^\perp$.
17. 设$V=\mathbb{R}^{2\times 2}$是实2×2矩阵的向量空间.
    (a) 确定双线性型$\langle A, B\rangle=\mathrm{trace}(AB)$关于标准基$\{e_{ij}\}$的矩阵.
    (b) 确定这个型的符号差.
    (c) 求这个型的一个正交基.
    (d) 确定这个型在V上的迹为零的矩阵子空间上的符号差.
*18. 求实$n\times n$矩阵的向量空间$\mathbb{R}^{n\times n}$上的型$\langle A, B\rangle=\mathrm{trace}(AB)$的符号差.
19. 设$V=\mathbb{R}^{2\times 2}$是2×2矩阵空间.
    (a) 证明由$\langle A, B\rangle=\det(A+B)-\det A-\det B$定义的型$\langle A, B\rangle$是对称的和双线性的.
    (b) 计算这个型关于标准基$\{e_{ij}\}$的矩阵并计算其符号差.
    (c) 对迹为零的矩阵的子空间作同样的计算.
20. 对于$\mathbb{R}^{3\times 3}$, 用A的特征多项式中t的系数代替双线性型$\det A$做练习19.
21. 决定复向量空间上对称型的西尔维斯特法则是什么, 并加以证明.
22. 用证明定理(2.9)的方法, 求出域F上每一个具有对称双线性型$\langle,\rangle$的有限维向量空间都有正交基的充分必要条件.
23. 设$F=\mathbb{F}_2$, 并设$A=\begin{bmatrix} & 1\\ 1 & \end{bmatrix}$.
    (a) 证明F^2上双线性型X^tAY不能对角化.
    (b) 求在系数属于F的2×2矩阵空间上$GL_2(F)$的作用P, $A \rightsquigarrow PAP^t$的轨道.

第三节 正定型相关的几何

1. 设V是欧几里得空间. 证明施瓦兹不等式和三角不等式.
2. 设W是欧几里得空间V的子空间. 证明$W=W^{\perp\perp}$.
3. 设V是欧几里得空间. 证明如果$|v|=|w|$, 则$(v+w)\perp(v-w)$. 给出这个公式的几何解释.

264

4. 在欧几里得空间中证明平行四边形法则$|v+w|^2+|v-w|^2=2|v|^2+2|w|^2$.
5. 证明正交投影(3.7)是线性变换.

6. 求使$\mathbb{R}^3$的标准基的象构成等边三角形且$\pi(e_1)$指向x-轴的方向的投影π：$\mathbb{R}^3\longrightarrow\mathbb{R}^2$的矩阵.

*7. 设W是$\mathbb{R}^3$的一个二维子空间，考虑$\mathbb{R}^3$到W上的正交投影π. 设$(a_i, b_i)^t$是$\pi(e_i)$关于选定的W的标准正交基的坐标向量. 证明(a_1, a_2, a_3)和(b_1, b_2, b_3)是正交的单位向量.

*8. 设$w\in\mathbb{R}^n$是一个长度为1的向量.

(a) 证明矩阵$P=I-2ww^t$是正交的.

(b) 证明用P左乘是一个通过空间W与w垂直的反射，即证明如果把任意一个向量写作$v=cw+w'$的形式，其中$w'\in W^{\perp}$，则$Pv=-cw+w'$.

(c) 设X, Y是$\mathbb{R}^n$中长度相同的任意向量. 求使$PX=Y$的向量w.

*9. 利用练习8证明每一个正交$n\times n$矩阵最多是n个反射的乘积.

10. 设A是一个实对称矩阵，T是$\mathbb{R}^n$中矩阵为A的线性算子.

(a) 证明$(\ker T)\perp(\operatorname{im}T)$且$V=(\ker T)\oplus(\operatorname{im}T)$.

(b) 证明T是到$\operatorname{im}T$上的正交投影当且仅当除了是对称以外还要求$A^2=A$.

11. 设A是对称的和正定的. 证明最大的矩阵元素在对角线上.

第四节　埃尔米特型

1. 验证法则(4.4).

2. 证明在$\mathbb{C}^n$中点积型$(X\cdot Y)=X^tY$不是正定的.

3. 证明矩阵A是埃尔米特的当且仅当相应的型X^*AX是埃尔米特的.

4. 证明如果对所有复向量X，X^*AX是实数，则A是埃尔米特的.

5. 证明$n\times n$埃尔米特矩阵构成一个实向量空间，求这个空间的一个基.

6. 设V是2-维埃尔米特空间. 令(v_1, v_2)是V的一个标准正交基. 刻画满足$v_1=v_1'$的所有的标准正交基(v_1', v_2').

7. 设$X, Y\in\mathbb{C}^n$是正交向量. 证明$|X+Y|^2=|X|^2+|Y|^2$.

8. $\mathbb{C}^2$上$\langle X, Y\rangle=x_1y_1+ix_1y_2-ix_2y_1+ix_2y_2$是埃尔米特型吗？

9. 设A, B是正定埃尔米特矩阵. 确定如下矩阵哪些是正定埃尔米特矩阵：A^2，A^{-1}，AB，$A+B$.

10. 证明埃尔米特矩阵的行列式是实数.

11. 证明A是正定埃尔米特矩阵当且仅当存在可逆酉矩阵P使得$A=P^*P$.

265

12. 证明定理(4.19)，即复向量空间V上的埃尔米特型有标准正交基当且仅当它是正定的.

13. 将正定的判别法(1.26)拓广到埃尔米特矩阵.

14. 对埃尔米特型叙述并证明西尔维斯特法则.

15. 设$\langle ,\rangle$是复向量空间V上的埃尔米特型，用$\{v, w\}$表示复数$\langle v, w\rangle$的实部. 证明如果将V视为实向量空间，则$\{,\}$是V上的一个对称双线性型. 且如果$\langle ,\rangle$正定，则$\{,\}$也正定. 对虚部你会有什么结论呢？

16. 设P是次数$\leqslant n$的多项式的向量空间.

(a) 证明

$$\langle f,g\rangle=\int_0^{2\pi}\overline{f(e^{i\theta})}g(e^{i\theta})d\theta$$

是P上的正定埃尔米特型.

(b) 求这个型的标准正交基.

17. 确定下列法则是否定义复矩阵空间$\mathbb{C}^{n\times n}$上的埃尔米特型，如果是的话确定其符号差.

(a) $A, B\rightsquigarrow\operatorname{trace}(A^*B)$　(b) $A, B\rightsquigarrow\operatorname{trace}(\overline{A}B)$

18. 设A是酉矩阵. 证明$|\det A|=1$.

19. 设P是酉矩阵，并设X_1，X_2是P的具有不同特征值λ_1，λ_2的特征向量. 证明X_1，X_2关于$\mathbb{C}^n$上的标准

埃尔米特积是正交的.

*20. 设 A 是任意复矩阵. 证明 $I+A^*A$ 非奇异.

21. 证明命题(4.20).

第五节 谱定理

1. 证明如果 T 是埃尔米特算子，则法则 $\{v, w\}=\langle v, Tw\rangle = X^* MY$ 定义 V 上的另一个埃尔米特型.

2. 证明实对称矩阵的特征值是实数.

3. 证明相应于埃尔米特矩阵 A 不同的特征值的特征向量正交.

4. 当

$$A=\begin{bmatrix} 1 & \mathrm{i} \\ -\mathrm{i} & 1 \end{bmatrix}$$

时求使 PAP^* 为对角矩阵的酉矩阵.

5. 当

(a) $A=\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$ (b) $A=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ (c) $A=\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

时，求使 PAP^t 为对角矩阵的实正交矩阵.

6. 证明谱定理中条件(b)与(a)的等价.

7. 证明实对称矩阵 A 正定当且仅当其特征值是正的.

8. 证明既是正定埃尔米特矩阵又是酉矩阵的矩阵只有单位矩阵.

9. 设 A 是实对称矩阵. 证明 e^A 是对称的和正定的.

10. 证明对任意方阵 A，$\ker A=(\operatorname{im}A^*)^{\perp}$.

*11. 设 $\xi=e^{2\pi i/n}$，并设 A 是 $n\times n$ 矩阵 $a_{jk}=\xi^{jk}/\sqrt{n}$. 证明 A 是酉矩阵.

12. 证明对每一复矩阵 A 存在酉矩阵 P 使得 PAP^* 是上三角的.

13. 设 A 是埃尔米特矩阵. 证明存在行列式为 1 的酉矩阵 P 使得 PAP^* 是对角的.

*14. 设 A，B 是交换的埃尔米特矩阵. 证明存在酉矩阵 P 使得 PAP^* 和 PBP^* 都是对角的.

15. 用谱定理给出对于某个 $n\times n$ 矩阵 A，正定实对称 $n\times n$ 矩阵 P 具有 $P=AA^t$ 的形式这一事实的一个新证明.

16. 设 λ，μ 是复对称矩阵 A 的不同的特征值，设 X，Y 是相应于这两个特征值的特征向量. 证明 X 与关于点积与 Y 正交.

第六节 圆锥曲线与二次曲面

1. 确定二次曲面 $x^2+4xy+2xz+z^2+3x+z-6=0$ 的类型.

2. 假设(6.1)代表一个椭圆. 除了先对角化然后再作平移而将型化为标准形式外，我们也可以先作平移. 说明如何用微积分计算所需的平移.

3. 讨论圆锥曲线的所有退化轨迹.

4. 用方程的系数给出一个圆锥曲线为圆的充分必要条件.

5. (a) 用二次型的符号差描述圆锥曲线的类型.

(b) 对 $\mathbb{R}^3$ 中的二次曲面做同样的描述.

6. 刻画退化二次曲面，即(6.14)中没有列出的那些.

第七节 正规算子的谱定理

1. 证明对任意正规矩阵 A，$\ker A=(\operatorname{im}A)^{\perp}$.

2. 证明或推翻：如果 A 是正规矩阵而 W 是 $V=\mathbb{C}^n$ 的一个 A-不变子空间，则 $W^{\perp}$ 也是 A-不变子空间.

266

3. 一个矩阵是斜埃尔米特的，如果 $A^*=-A$. 关于这样的矩阵的特征值和对角化的可能性你有什么结论？

4. 证明循环移位算子

$$\begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & & \ddots & 1 \\ 1 & & & & 0 \end{bmatrix}$$

是正规的，并确定其对角化.

5. 设 P 为一个正规的具有实特征值的实矩阵. 证明 P 是对称的.

267 6. 设 P 是一个实的斜对称矩阵. 证明 P 是正规的.

*7. 证明循环矩阵

$$\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_n \\ c_n & c_0 & c_1 & \cdots & c_{n-1} \\ \vdots & & & & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}$$

是一个正规矩阵.

8. (a) 设 A 是一个复对称矩阵. 证明 A 的有不同特征值的特征向量关于双线性型 X^tX 是正交的.

*(b) 举出一个复对称矩阵 A 的例子，使得没有使 PAP^t 为对角矩阵的 $P\in O_n(\mathbb{C})$.

9. 设 A 是一个正规矩阵. 证明 A 是埃尔米特的当且仅当 A 的特征值是实的，而 A 是酉的当且仅当每个特征值的绝对值为 1.

10. 设 V 是具有正定埃尔米特型 $\langle,\rangle$ 的有限维复向量空间，并设 $T: V\longrightarrow V$ 是 V 上的线性算子. 设 A 是 T 关于一个标准正交基 $\boldsymbol{B}$ 的矩阵. 伴随算子 $T^*: V\to V$ 定义为关于同一标准正交基的矩阵为 A^* 的算子.

(a) 证明对所有 $v, w\in V$，T 和 T^* 由等式 $\langle Tv, w\rangle=\langle v, T^*w\rangle$ 及 $\langle v, Tw\rangle=\langle T^*v, w\rangle$ 联系起来. 证明这两个等式中的第一个刻画了 T^*.

(b) 证明 T^* 与标准正交基的选择无关.

(c) 设 v 是 T 的具有特征值 λ 的特征向量，设 $W=v^\perp$ 是与 v 正交的向量空间. 证明 W 是 T^*-不变的.

11. 证明对任意线性算子 T，TT^* 是埃尔米特的.

12. 设 V 是具有正定埃尔米特型 $\langle,\rangle$ 的有限维复向量空间. 线性算子 $T: V\to V$ 称为**正规的**，如果 $TT^*=T^*T$.

(a) 证明 T 是正规的当且仅当对所有 $v, w\in V$，$\langle Tv, Tw\rangle=\langle T^*v, T^*w\rangle$，并验证埃尔米特算子和酉算子是正规的.

(b) 假设 T 是正规算子，并设 v 是 T 的具有特征值 λ 的特征向量. 证明 v 也是 T^* 的特征向量并求其特征值.

(c) 证明若 v 是 T^* 的特征向量，则 $W=v^\perp$ 是 T-不变的，由此证明正规算子的谱定理.

第八节　斜对称型

1. 证明或推翻：矩阵 A 是斜对称的当且仅当对所有 X，$X^tAX=0$.

2. 证明一个型是斜对称的当且仅当其矩阵具有性质(8.4).

3. 证明或推翻：当 n 为奇数时斜对称 $n\times n$ 矩阵是奇异的.

4. 证明或推翻：一个实的斜对称矩阵的特征值是纯虚数.

*5. 设 S 是实的斜对称矩阵. 证明 $I+S$ 可逆，并且 $(I-S)(I+S)^{-1}$ 是正交的.

*6. 设 A 是实的斜对称矩阵.

(a) 证明 $\det A\geqslant 0$.

268

(b) 证明：如果 A 的元素都是整数，则 $\det A$ 是整数的平方.

7. 设 $\langle , \rangle$ 是向量空间 V 的斜对称型. 如第二节那样定义正交性、迷向空间和非退化型.

(a) 证明型非退化当且仅当它关于任一个基的矩阵是非奇异的.

(b) 设 W 是子空间且型在 W 上的限制非退化，则 $V=W\oplus W^{\perp}$.

(c) 证明如果型不恒等于零，则存在 V 的子空间 W 及 W 的一个基，使得型在 W 上的限制的矩阵为 $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

(d) 证明定理(8.6).

第九节　用矩阵记号对结果的小结

1. 在下列情形中确定矩阵 $AB+BA$ 和 $AB-BA$ 是否对称.

(a) A，B 对称　(b) A，B 埃尔米特　(c) A，B 斜对称　(d) A 对称 B 斜对称

2. 说出下列规则中哪个定义了 $GL_n(\mathbb{C})$ 在所有复矩阵的空间 $\mathbb{C}^{n\times n}$ 上的作用：

$$P,A \rightsquigarrow PAP^t,\quad (P^{-1})^t A(P^{-1}),\quad (P^{-1})^t AP^t, P^{-1}AP^t,\quad AP^t, P^tA.$$

3. (a) 对以下每一类矩阵，描述可能的行列式：

(i) 实正交　(ii) 复正交　(iii) 酉的　(iv) 埃尔米特的

(v) 辛的　(vi) 实对称的，正定　(vii) 实对称的，负定

(b) 这些类型的矩阵中哪些具有实特征值？

4. (a) 设 E 是任意复矩阵. 证明矩阵 $\begin{bmatrix} I & E^* \\ -E & I \end{bmatrix}$ 是可逆的.

(b) 以块的形式 $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ 求出其逆.

*5. (a) 下列论证有什么错误？设 P 是实正交矩阵. 设 X 是 P 的(可能是复的)特征向量，特征值为 λ. 则 $X^tP^tX=(PX)^tX=\lambda X^tX$. 另一方面，$X^tP^tX=X^t(P^{-1}X)=\lambda^{-1}X^tX$. 因此 $\lambda=\lambda^{-1}$，于是 $\lambda=\pm 1$.

(b) 基于这个论证叙述并证明正确的定理.

*6. 说明如何用 $\mathbb{R}^4$ 中两个正交平面的旋转描述 SO_4 中的任意元素.

*7. 设 A 是实 $m\times n$ 矩阵. 证明存在正交矩阵 $P\in O_m$ 和 $Q\in O_n$ 使得 $PAQ=D$ 是有非负对角元的对角矩阵.

269

第八章 线 性 群

在这些日子里，拓扑学的天使和抽象代数的恶魔
为争夺每一个数学方向的灵魂进行着斗争.

Hermann Weyl

第一节 典型线性群

一般线性群 GL_n 的子群称为**线性群**. 本章将研究其中最重要的那些：正交群、酉群及辛群. 它们称为**典型群**.

典型群作为 GL_n 在 $n\times n$ 矩阵空间自然作用的稳定子出现. 这些作用的第一个是描述一个双线性型中基变换的那个. 规则

【1.1】 $$P, A \rightsquigarrow (P^t)^{-1}AP^{-1}$$

是 GL_n 在所有 $n\times n$ 矩阵的集合上的作用. 这在任意的标量域上都成立，但我们感兴趣的是实的和复的情形. 如在第七章(1.15)所见到的，矩阵 A 在这个作用下的轨道是代表型 X^tAX 关于不同的基的矩阵 A' 的集合. 习惯上把同一个轨道中的矩阵称为**相合的**. 可以令 $Q=(P^t)^{-1}$ 而得到等价的定义

【1.2】 A 与 A' *相合，如果对某个* $Q\in GL_m(F)$ *有* $A'=QAQ^t$.

西尔维斯特法则[第七章(2.11)]描述了实对称矩阵不同的轨道或相合类. 每一个实对称矩阵的相合类恰好含有一个形如第七章(2.10)的矩阵. 前面定义的**正交群**是在这个作用下恒等矩阵的稳定子. 同前面一样，我们用符号 O_n 表示实正交群：

270

【1.3】 $$O_n = \{P \in GL_n(\mathbb{R}) \mid P^tP = I\}.$$

复正交群可以类似地定义：

$$O_n(\mathbb{C}) = \{P \in GL_n(\mathbb{C}) \mid P^tP = I\}.$$

由矩阵

$$I_{3,1} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}$$

定义的**洛伦兹型**[第七章(2.16)]的稳定子称为**洛伦兹群**. 记为 $O_{3,1}(\mathbb{R})$或 $O_{3,1}$：

【1.4】 $$O_{3,1} = \{P \in GL_n(\mathbb{R}) \mid P^tI_{3,1}P = I_{3,1}\}.$$

由这些矩阵所代表的线性算子常称为**洛伦兹变换**. 下标(3.1)表示矩阵的符号差，即+1 和−1 的个数. 用这种方式对任意符号差(p, q)可定义一个类似的群 $O_{p,q}$.

作用(1.1)亦描述了不是对称的型的基变换. 这样第七章的定理(8.6)告诉我们：

【1.5】推论 *若 m 为偶数，则恰好存在一个实的非退化斜对称 $m\times m$ 矩阵的相合类.* ■

标准斜对称型由 $2n\times 2n$ 矩阵 J 定义(第七章(8.5))，其稳定子称为辛群

【1.6】
$$SP_{2n}(\mathbb{R}) = \{P \in GL_{2n}(\mathbb{R}) \mid P^t JP = J\}.$$

同样，复辛群 $SP_{2n}(\mathbb{C})$也类似地定义.

最后，酉群通过作用

【1.7】
$$P, A \rightsquigarrow (P^*)^{-1}AP^{-1}$$

来定义. 只有当标量域是复数域时这个定义才有意义. 与双线性型完全一样，矩阵 A 的轨道由关于不同的基定义型$\langle X, Y\rangle = X^*AY$的矩阵组成(见[第七章(4.12)]). 酉群是在这个作用下单位矩阵的稳定子：

【1.8】
$$U_n = \{P \mid P^*P = I\}.$$

这样 U_n 是代表使埃尔米特点积[第七章(4.2)]X^*Y 不变的基变换的矩阵的群.

加上特殊一词来描述行列式为 1 的矩阵子群. 这样我们得到更多的群：

特殊线性群 $SL_n(\mathbb{R})$：行列式为 1 的 $n\times n$ 矩阵 P；
特殊正交群 $SO_n(\mathbb{R})$：交 $SL_n(\mathbb{R})\cap O_n(\mathbb{R})$；
特殊酉群 SU_n：交 $SL_n(\mathbb{C})\cap U_n$.

虽然由定义看不出来，但辛矩阵的行列式总是为 1，因而在两个记号中使用 S 并不会产生矛盾.

第二节 特殊酉群 SU_2

本章的主要目的是通过把典型线性群作为所有矩阵构成的空间$\mathbb{R}^{n\times n}$或$\mathbb{C}^{n\times n}$的子集来考虑，从而描述它们的几何性质. 我们已经知道一些群的几何. 例如，$GL_1(\mathbb{C}) = \mathbb{C}^\times$ 是“带孔平面”$\mathbb{C}-\{0\}$. 还有，如果 p 是 1×1 矩阵，则 $p^* = \bar{p}$. 这样

【2.1】
$$U_1 = \{p \in \mathbb{C}^\times \mid \bar{p}p = 1\}.$$

这是绝对值为 1 的复数的集合——复平面上的单位圆. 可通过映射 $x_1 + x_2 i \rightsquigarrow (x_1, x_2)$，将它等同于$\mathbb{R}^2$ 中的单位圆，

$$x_1^2 + x_2^2 = 1.$$

平面旋转群 SO_2 同构于 U_1. 它也是圆，通过映射

【2.2】
$$(x_1, x_2) \rightsquigarrow \begin{bmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{bmatrix}$$

嵌入$\mathbb{R}^{2\times 2}$. 在以后各节我们将描述更多的群.

粗略地说，线性群 G 的维数是 G 中矩阵自由度的个数. 例如，群 SO_2 的维数是 1. SO_2 中一个矩阵代表一个转过角度 θ 的旋转，这个角度是确定旋转所需要的单独一个参数. 在第七节里将更仔细地讨论维数，但首先具体地描述一些低维群. 真正有意义的群的最小维数是 3，其中三个群——SU_2，SO_3 和 $SL_2(\mathbb{R})$——是非常重要的. 本节我们将研究特殊酉群 SU_2.

设 $P=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$是 SU_2 的一个元素，其中 $a, b, c, d\in\mathbb{C}$. 定义 SU_2 的等式是 $P^*P=I$ 且

271

$\det P=1$. 由克莱姆法则，

$$P^{-1}=(\det P)^{-1}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}=\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

由于对 SU_2 中的每个矩阵有 $P^{-1}=P^*$，我们得到 $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}=\begin{bmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{bmatrix}$，或者说

【2.3】
$$\bar{a}=d,\quad \bar{b}=-c.$$

这样

272

【2.4】
$$P=\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}.$$

需要把在计算中失去的条件 $\det P=1$ 找回来：

【2.5】
$$\bar{a}a+\bar{b}b=1.$$

等式(2.3)和(2.5)给出了描述 SU_2 中矩阵的元素的完整条件. 矩阵 P 由长度为 1 的向量 $(a, b)\in\mathbb{C}^2$ 刻画，且任意这样的向量由规则(2.4)给出一个矩阵 $P\in SU_2$.

如果用其实部和虚部写出 a, b，则等式(2.5)给出一个 SU_2 与$\mathbb{R}^4$ 中位于

【2.6】
$$x_1^2+x_2^2+x_3^2+x_4^2=1$$

的轨迹中的点的一一对应. 如果令 $a=x_1+x_2\mathrm{i}$ 及 $b=x_3+x_4\mathrm{i}$，则这个等式等价于(2.5).

类似于$\mathbb{R}^3$ 中的单位球面，轨迹(2.6)称为$\mathbb{R}^4$ 中的单位 3-球面. 数 3 指其维数，也就是球面中点的自由度的个数. 这样$\mathbb{R}^3$ 中的单位球面

$$x_1^2+x_2^2+x_3^2=1$$

作为曲面，称为 2-球面. $\mathbb{R}^2$ 的单位圆是一条曲线，称为 1-球面. 我们有时记一个 d 维球面为 S^d.

欧几里得空间子集间的双射 f: $S\longrightarrow S'$称为同胚，如果 f 与 f^{-1}都是连续映射(附录第三节). 将 SU_2 视为$\mathbb{C}^{2\times 2}$的子集，它与球面(2.6)间的对应显然是连续的，其逆亦然. 因而两个空间是同胚的.

【2.7】 SU_2 与$\mathbb{R}^4$ 中单位 3-球面同胚.

将 SU_2 与单位 3-球面等同起来会很方便. 如果将矩阵(2.4)用其顶行，也就是向量$(a, b)\in\mathbb{C}^2$ 表示，或用向量$(x_1, x_2, x_3, x_4)\in\mathbb{R}^4$ 表示，我们就得到这样的等同. 这些表示可认为是群的同一元素 P 的不同记号，且可以由一个换到另一个. 从几何的可视角度讲，表示 $P=(a, b)$和 $P=(x_1, x_2, x_3, x_4)$由于维数低，会更方便.

3-球面具有群结构这一事实是非常值得注意的，因为无法把 2-球面做成具有连续的合成法则的群. 事实上一个著名的拓扑定理断言，具有连续的群法则的球面只有实现为旋转群 SO_2 的 1-球面和 3-球面 SU_2.

现在将描述 SU_2 的类似于 2-球面上有常值经纬的曲线的代数结构. 矩阵 I, $-I$ 将扮演北极和南极的角色. 用我们的向量记号，它们是球面上的点$(\pm1, 0, 0, 0)$.

如果 2-球面 $x_1^2+x_2^2+x_3^2=1$ 的极点放在点$(\pm1, 0, 0)$，则纬为圆 $x_1=c$, $-1<c<1$. 3-球面 SU_2 上有类似纬的 x_1 坐标为常数的曲面. 它们是二维球面，通过

【2.8】 $$x_1 = c \quad \text{且} \quad x_2^2 + x_3^2 + x_4^2 = (1-c^2), -1 < c < 1$$ 273

嵌入$\mathbb{R}^4$. 这些集合可以代数地描述为 SU_2 中的共轭类

【2.9】命题 除了两种特殊情形，SU_2 的共轭类都是纬，即由方程(2.8)定义的集合. 对于区间$(-1, 1)$中的 c，这个集合由迹 $\text{trace}P=2c$ 的所有矩阵 $P\in SU_2$ 组成. 剩下的共轭类是$\{I\}$和$\{-I\}$，每个由一个元素组成. 这两个类构成群 SU_2 的中心 $Z=\{\pm I\}$.

证明 矩阵 P(2.4)的特征多项式是

【2.10】 $$t^2-(a+\bar{a})t+1=t^2-2x_1t+1.$$

这个多项式在单位圆上有一对复共轭根 λ，$\bar{\lambda}$，它们是 P 的特征值，仅与迹 $\text{trace}P=2x_1$ 有关. 更进一步，迹不相同的两个矩阵有不同的特征值. 如果能够证明 P 的共轭类包含 SU_2 中每一个具有相同特征值的矩阵，我们就得到了命题. $x_1=1$，-1 的情形对应于两个特殊的共轭类$\{I\}$和$\{-I\}$,这样命题的证明由下面的引理完成.

【2.11】引理 设 P 是 SU_2 中一个元素，其特征值为 λ，$\bar{\lambda}$. 则 P 在 SU_2 中共轭于矩阵

$$\begin{bmatrix}\lambda & \\ & \bar{\lambda}\end{bmatrix}.$$

证明 由正规算子的谱定理[第七章(7.3)]，存在酉矩阵 Q 使得 QPQ^* 为对角矩阵. 我们只需证明可选择 Q 使其行列式为 1 就行了. 设 $\det Q=\delta$. 因为 $Q^*Q=1$，$\det(Q^*)\det(Q)=\bar{\delta}\delta=1$；因此 δ 的绝对值为 1. 设 ϵ 为 δ 的平方根，则亦有$\bar{\epsilon}\epsilon=1$. 矩阵 $Q_1=\bar{\epsilon}Q$ 属于 SU_2，且 $P_1=Q_1PQ_1{}^*$ 也是对角的. P_1 的对角元素是特征值λ，$\bar{\lambda}$. 矩阵

【2.12】 $$Q_2=\begin{bmatrix} & 1\\ -1 & \end{bmatrix}$$

也是 SU_2 的一个元素，必要时通过用这个矩阵作共轭，可以互换两个特征值. ■

接下来将引入 SU_2 的经. 2-球面 $x_1^2+x_2^2+x_3^2=1$ 上的经可以刻画为球面与包含两个极点$(\pm1, 0, 0)$的平面之交. 当加上第四个变量 x_4 而得到 3-球面时的方程，拓广这一定义的自然方式是构造与$\mathbb{R}^4$ 中包含两个极点$\pm I$ 的二维子空间的交. 这是 SU_2 中的一个圆，我们将把这些圆视为经. 这样虽然 SU_2 的纬是 2-球面，其经却是 1-球面，是过极点的“最大的圆”.

注意除了极点外，SU_2 的每个点 $P=(x_1, x_2, x_3, x_4)$恰好包含在一个经之中. 这是因为如果 P 不是极点，则 P 与 I 线性无关，这样它们可以张成$\mathbb{R}^4$ 的一个二维子空间 V. 交 $SU_2\cap V$ 是包含 P 的唯一的经. 274

SU_2 与由 $x_3=x_4=0$ 定义的平面 W 的交是一个特别漂亮的经. 使用矩阵记号时，这个大圆由 SU_2 中的对角矩阵构成，它们构成一个子群 T:

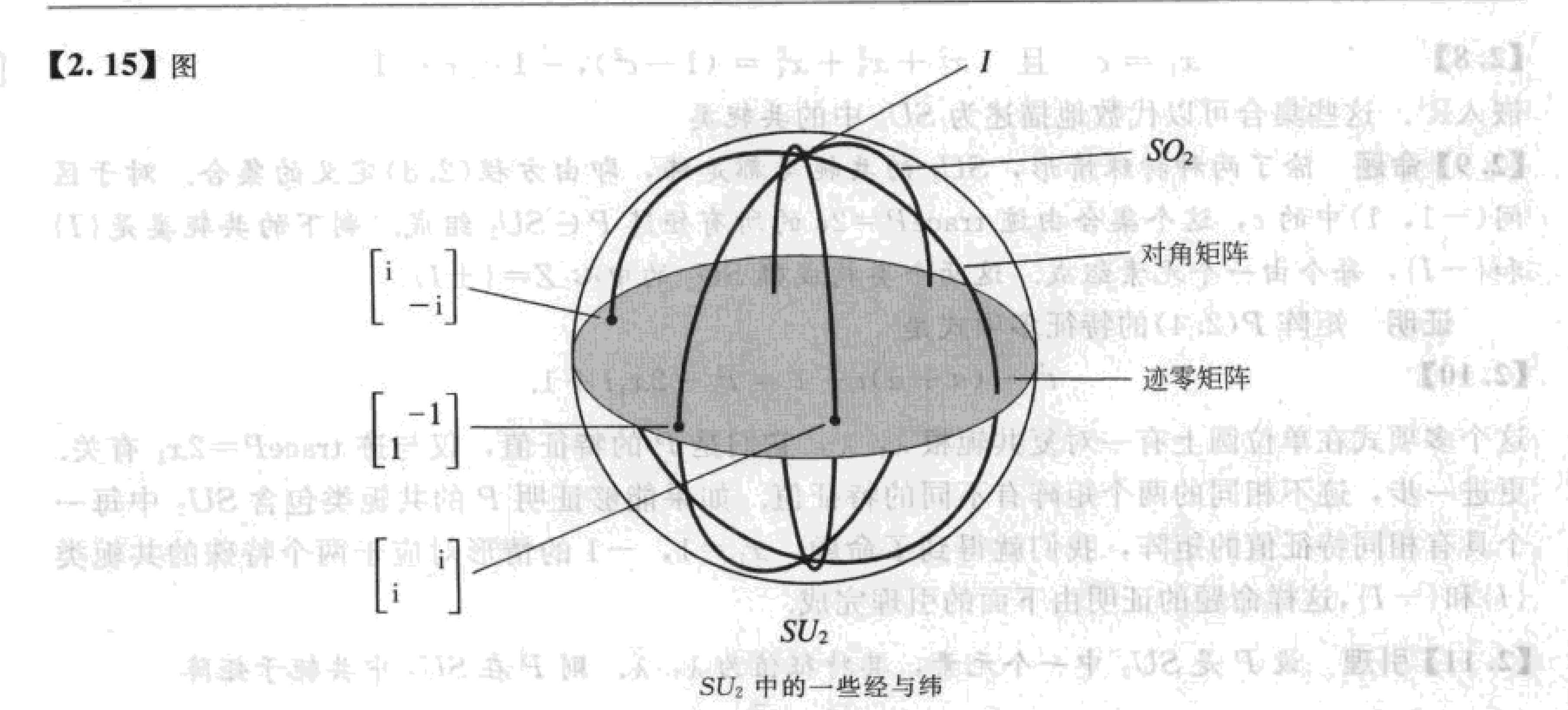
【2.13】 $$T=\left\{\begin{bmatrix}\lambda & \\ & \bar{\lambda}\end{bmatrix}\middle|\lambda\bar{\lambda}=1\right\}.$$

下面的命题刻画其他经.

【2.14】命题 SU_2 的经是子群 T 的共轭子群 QTQ^*.

273

【2.15】图



SU_2 中的一些经与纬

在图(2.15)中 3-球面 SU_2 从$\mathbb{R}^4$ 投影到平面上的单位圆盘. 所示的共轭类是$\mathbb{R}^4$ 的"赤道"纬，它由方程 $x_1=0$ 定义. 就像一个圆由$\mathbb{R}^3$ 到$\mathbb{R}^2$ 的正交投影是椭圆一样，这个 2-球面从$\mathbb{R}^4$ 到$\mathbb{R}^3$ 的正交投影是椭球面，而这个椭球面在平面上的进一步投影是所示的椭圆盘.

命题(2.14)的证明 这里的要点是证明任意共轭子群 QTQ^* 是经. 引理(2.11)告诉我们每个元素 $P\in SU_2$ 位于这些共轭子群之一中(虽然 Q 与 Q^* 的角色已互换). 因为每个 $P\neq\pm I$ 恰好含于一个经中，从而得到每一个经是子群 QTQ^* 之一.

我们来证明共轭子群 QTQ^* 是经. 这个事实成立的原因是：由一个固定元素 Q 给出的共轭是一个线性算子，它将子空间 W 映到另一个子空间. 具体地计算共轭就可以搞清楚这一点. 设 Q 是矩阵(2.4). 设 $w=(w_1, w_2, 0, 0)$表示 W 的一个变元，且令 $z=w_1+w_2\mathrm{i}$. 于是

275

$$\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}\begin{bmatrix} z & \\ & \bar{z} \end{bmatrix}\begin{bmatrix} \bar{a} & -b \\ \bar{b} & a \end{bmatrix}=\begin{bmatrix} a\bar{a}z+b\bar{b}\bar{z} & ab(\bar{z}-z) \\ * & * \end{bmatrix}.$$

计算这些元素，我们发现 w 被映为向量 $u=(u_1, u_2, u_3, u_4)$，其中

$$u_1=w_1, u_2=(x_1^2+x_2^2-x_3^2-x_4^2)w_2,$$
$$u_3=2(x_1x_4+x_2x_3)w_2, u_4=2(x_2x_4-x_1x_3)w_2.$$

坐标 u_i 是(w_1, w_2)的实线性组合. 这证明了映射 $w \rightsquigarrow u$ 是实线性变换. 故其象 V 是$\mathbb{R}^4$ 的子空间. 共轭群 QTQ^* 为 $SU_2\cap V$. 因为 QTQ^* 包含两极$\pm I$，故 V 亦包含$\pm I$，这表明 QTQ^* 是一个经. ■

我们将简略地描述另一个几何构造：如我们所见，对角矩阵的子群 T 是 3-球面 SU_2 中的大圆. 这个子群的左陪集，也就是形如 $QT(Q\in SU_2)$的集合也是大圆，且它们划分了群 SU_2. 这样 3-球面划分为大圆. 这个非常有趣的结构称为霍普夫纤维化.

第三节 SU_2 的正交表示

上一节我们看到特殊酉群 SU_2 的共轭类是二维球面. 由于共轭类是共轭作用的轨道，故 SU_2 在这些球面上作用. 本节将证明由元素 $P\in SU_2$ 的共轭在每个球面上作用为一个旋转，并

且将 P 映到这个旋转的矩阵的映射定义了一个满同态

【3.1】
$$\varphi: SU_2 \longrightarrow SO_3,$$

其核为 SU_2 的中心 $Z=\{\pm I\}$. 这个同态称为 SU_2 的*正交表示*. 它用一个实 3×3 旋转矩阵 $\varphi(P)$ 来代表 SU_2 中的一个复 2×2 矩阵 P.

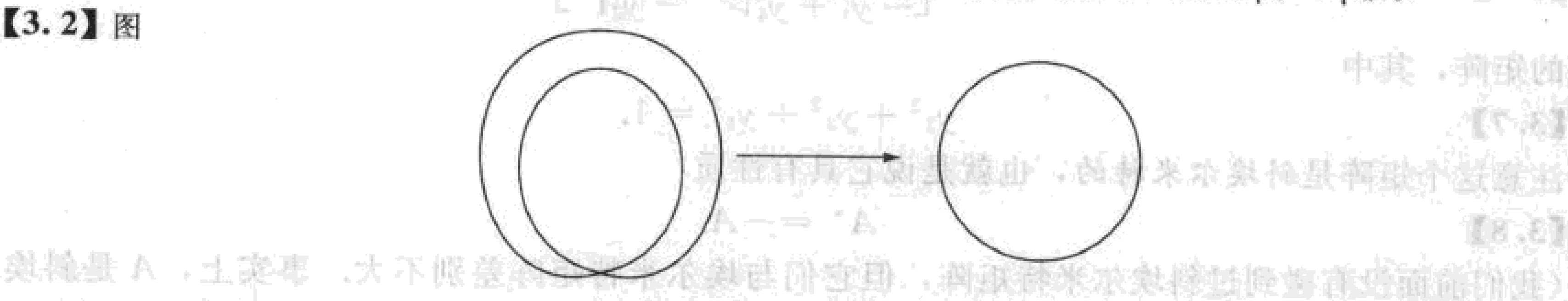
证明 P 通过旋转共轭类来作用的最保险的方式也许是直接写下代表旋转的矩阵. (3.12) 就是这样做的. 然而, $\varphi(P)$ 的公式比较复杂并且没有什么启发性. 最好是间接地描述 φ, 这是我们目前要做的. 首先讨论映射的几何.

由于 φ 的核是 $\{\pm I\}$, 其陪集是集合 $\{\pm P\}$. 它们构成同态的纤维. 因而 SO_3 的每个元素对应于一对相差一个符号的酉矩阵. 由此, 群 SU_2 称为群 SO_3 的*双重覆盖*.

276

由 $\rho_\theta \rightsquigarrow \rho_{2\theta}$ 定义的 1-球面到自身的映射 μ: $SO_2 \longrightarrow SO_2$ 是另一个双重覆盖的例子. 其核也由两个元素, 即恒等和转过 π 的旋转组成. μ 的每个纤维包含两个旋转 ρ_θ 和 $\rho_{\pi+\theta}$.

【3.2】 图



1-球面的一个双重覆盖

正交表示可用于确定旋转群的拓扑结构. 使用向量记号, 如果 $P=(x_1, \cdots, x_4)$, 则 $-P=(-x_1, \cdots, -x_4)$, 点 $-P$ 称为点 P 的*对极*. 于是由于旋转群的点对应于陪集 $\{\pm P\}$, 故群 SO_3 可由在 3-球面上等同对极的点而得到. 以这种方式得到的空间称为*实射影 3-空间*:

【3.3】 *SO_3 同胚于实射影 3-空间.*

这里数 3 也是指空间的维数. 实射影 3-空间的点也与 $\mathbb{R}^4$ 中过原点的直线(或一维子空间)一一对应. 每一过原点的直线与单位球面交于一对对极点.

如我们在第四章第八节所见到的, SO_3 除恒等映射外每个元素可由一个对 (v, θ) 来描述, 其中 v 是旋转轴上的单位向量而 θ 是旋转的角度. 然而, 两个对 (v, θ) 和 $(-v, -\theta)$ 代表同一个旋转. 物理学家把从这两个对之中选择一个称作*自旋*的选择. 要选出在整个群上连续变化的自旋是不可能的. 两个可能的选择反而定义了 $SO_3-\{I\}$ 的一个双重覆盖. 我们可以把所有对 (v, θ) 的集合通过积空间 $S\times\Theta$ 来实现, 其中 S 是 $\mathbb{R}^3$ 中单位向量的 2-球面, 而 Θ 是非零角度 $0<\theta<2\pi$ 的集合. 这个积空间映射到 SO_3:

【3.4】
$$\psi: S\times\Theta \longrightarrow SO_3-\{I\},$$

把 (v, θ) 映到绕 v 转过角度 θ 的旋转. 因为每个非平凡的旋转与两个对 (v, θ) 和 $(-v, -\theta)$ 相伴, 所以映射 ψ 是 $SO_3-\{I\}$ 的一个双重覆盖.

我们现在有 $SO_3-\{I\}$ 的两个双重覆盖, 即 $S\times\Theta$ 及 $SU_2-\{\pm I\}$, 想必它们是等价的. 这是对的:

【3.5】命题 *存在同胚 h: $(SU_2-\{\pm I\}) \longrightarrow S\times\Theta$, 它与到 SO_3 的映射相容, 即使得 $\psi\circ h=\varphi$.*

277

这个映射 h 不是群同态. 事实上其定义域及其值域都不是群.

命题(3.5)不是太难证明，但因为有两个这样的同胚，证明有点难懂. 它们差一个自旋的交换. 另一方面，因为空间 $SU_2-\{\pm I\}$ 是单连通的，这个同胚的存在可由拓扑学的一个一般定理得到.（单连通空间是路连通的并且其中每一个圈可以连续地收缩到一个点的空间.）最好是将其证明留给拓扑学家.

因此，除了 $\pm I$ 外，SU_2 的每个元素可以描述为 $\mathbb{R}^3$ 中加上了一个自旋选择的旋转. 由此 SU_2 常被称为*自旋群*.

我们现在着手计算同态 φ，必须选定一个共轭类来开始. 选择 SU_2 中一个由迹零矩阵组成的类会方便些，它是由 $x_1=0$ 定义并且如图(2.15)所示. 在其他类上群以相同的方式作用. 我们将迹零矩阵的共轭类称为 C. 则 C 的一个元素 A 将是形如

【3.6】
$$A=\begin{bmatrix} y_2\mathrm{i} & y_3+y_4\mathrm{i} \\ -y_3+y_4\mathrm{i} & -y_2\mathrm{i}\end{bmatrix}$$

的矩阵，其中

【3.7】
$${y_2}^2+{y_3}^2+{y_4}^2=1.$$

注意这个矩阵是*斜埃尔米特*的，也就是说它具有性质

【3.8】
$$A^*=-A.$$

（我们前面没有碰到过斜埃尔米特矩阵，但它们与埃尔米特矩阵差别不大. 事实上，A 是斜埃尔米特矩阵当且仅当 $H=\mathrm{i}A$ 是埃尔米特矩阵.）迹为零的 2×2 斜埃尔米特矩阵构成一个三维实向量空间 V，它的基为

【3.9】
$$\boldsymbol{B}=\left[\begin{bmatrix}\mathrm{i} & \\ & -\mathrm{i}\end{bmatrix},\begin{bmatrix} & 1\\ -1 & \end{bmatrix},\begin{bmatrix} & \mathrm{i}\\ \mathrm{i} & \end{bmatrix}\right].$$

利用(3.6)的记号，有 $A=\boldsymbol{B}Y$，其中 $Y=(y_2,\ y_3,\ y_4)^t$. 因而基 $\boldsymbol{B}$ 对应于空间 $\mathbb{R}^3$ 的标准基$(e_2,\ e_3,\ e_4)$，(3.7)告诉我们共轭类表示为这个空间中的单位球面.

注意 SU_2 通过共轭不仅仅作用在其单位球面上，而且也作用在整个迹零的斜埃尔米特矩阵空间上：如果 $A\in V$，$P\in SU_2$，且如果有 $B=PAP^*=PAP^{-1}$，则 $\mathrm{trace}B=0$，并且 $B^*=(PAP^*)^*=PA^*P^*=P(-A)P^*=-B$. 还有，因为 $P(A+A')P^*=PAP^*+PA'P^*$，且如果 r 是实数，则$P(rA)P^*=rPAP^*$，所以给定矩阵 P 的共轭给出一个 V 上的线性算子. 这个线性算子的矩阵定义为 $\varphi(P)$. 要具体求出这个矩阵，我们用 P 做基(3.7)的共轭并将结果用这个基重新表出. 例如，

278

【3.10】
$$\begin{bmatrix} a & b\\ -\bar b & \bar a\end{bmatrix}\begin{bmatrix}\mathrm{i} & \\ & -\mathrm{i}\end{bmatrix}\begin{bmatrix}\bar a & -b\\ \bar b & a\end{bmatrix}=\mathrm{i}\begin{bmatrix} a\bar a-b\bar b & -2ab\\ -2\bar a\bar b & b\bar b-a\bar a\end{bmatrix}.$$

这个矩阵的坐标是 $y_2=a\bar a-b\bar b$，$y_3=\mathrm{i}(-ab+\bar a\bar b)$和 $y_4=-(ab+\bar a\bar b)$. 它们构成矩阵 $\varphi(P)$ 的第一列. 类似地计算其余各列得到

【3.11】
$$\begin{bmatrix} (a\bar a-b\bar b) & \mathrm{i}(\bar a b-a\bar b) & (\bar a b+a\bar b)\\ \mathrm{i}(\overline{ab}-ab) & \frac{1}{2}(a^2+\bar a^2+b^2+\bar b^2) & \frac{\mathrm{i}}{2}(a^2-\bar a^2-b^2+\bar b^2)\\ -(\overline{ab}+ab) & \frac{\mathrm{i}}{2}(\bar a^2-a^2+\bar b^2-b^2) & \frac{1}{2}(a^2+\bar a^2-b^2-\bar b^2)\end{bmatrix}.$$

我们将不会用到上面的计算. 即使没有这个计算，我们也知道 $\varphi(P)$ 是个实的 3×3 矩阵，这是因为它是一个三维实向量空间的线性算子的矩阵.

【3.12】引理 映射 $P \rightsquigarrow \varphi(P)$ 定义一个同态 $SU_2 \longrightarrow GL_3(\mathbb{R})$.

证明 由共轭作用的结合律[第五章(5.1)]得到 φ 与乘法是相容的：乘积 PQ 在矩阵 A 上的作用为 $(PQ)A(PQ)^*=P(QAQ^*)P^*$. 这是由 P 的和由 Q 的共轭作用的合成. 由于线性算子的合成的矩阵是矩阵的乘积，$\varphi(PQ)=\varphi(P)\varphi(Q)$. 由于与乘法相容，$\varphi(P^{-1})\varphi(P)=\varphi(I_2)=I_3$. 所以对每个 P，$\varphi(P)$ 可逆，因而，正如所断言的，φ 是由 SU_2 到 $GL_3(\mathbb{R})$ 的一个同态. ■

【3.13】引理 对任意 P，$\varphi(P)\in SO_3$. 因此 $P \rightsquigarrow \varphi(P)$ 定义一个同态 $SU_2 \longrightarrow SO_3$.

证明 可以用公式(3.11)证明这个引理. 要从概念上来证明它，我们注意到 $\mathbb{R}^3$ 上的点积在 V 上是一个双线性型并且有一个漂亮的矩阵表达式. 用(3.6)的记号，定义 $\langle A, A'\rangle = y_2y_2'+y_3y_3'+y_4y_4'$. 则有

【3.14】
$$\langle A,A'\rangle = -\frac{1}{2}\operatorname{trace}(AA').$$

这可通过计算证明：

$$AA'=\begin{bmatrix} -(y_2y_2'+y_3y_3'+y_4y_4')+(y_3y_4'-y_4y_3')\mathrm{i} & * \\ * & -(y_2y_2'+y_3y_3'+y_4y_4')-(y_3y_4'-y_4y_3')\mathrm{i}\end{bmatrix},$$

所以 $\operatorname{trace}(AA')=-2\langle A, A'\rangle$.

点积的这个表达式表明它在由一个元素 $P\in SU_2$ 所作的共轭下保持不变：

$$\langle PAP^*,PA'P^*\rangle = -\frac{1}{2}\operatorname{trace}(PAP^*PA'P^*) = -\frac{1}{2}\operatorname{trace}(AA') = \langle A,A'\rangle.$$

或者用坐标向量来说，有 $(\varphi(P)Y\cdot\varphi(P)Y')=(Y\cdot Y')$. 由此得到 $\varphi(P)$ 位于正交群 $O_3=O_3(\mathbb{R})$ [第四章(5.13)].

为完成证明，我们验证对每个 $P\in SU_2$，$\varphi(P)$ 的行列式为 1：作为球面，SU_2 是路连通的. 由连续函数 $\det\varphi(P)$，它只能取两个可能值 ±1 中的一个. 因为 $\varphi(I_2)=I_3$ 而 $\det I_3=1$，它的值总是 $+1$，并且 $\varphi(P)\in SO_3$，这正是要证的. ■

【3.15】引理 $\ker\varphi=\{\pm I\}$.

证明 φ 的核由在 V 上平凡作用的矩阵 $P\in SU_2$ 组成，也就是说对所有迹零斜对称埃尔米特矩阵都有 $PAP^*=A$. 假定 P 对所有 $A\in V$ 具有性质 $PAP^*=A$，或 $PA=AP$. 我们在基(3.7)上进行检验. 由检验得到 $b=0$，$a=\bar{a}$，这给出 $P=\pm I$ 这两种可能，并且它们都属于核. 因而正如所断言的，$\ker\varphi=\{\pm I\}$. ■

【3.16】引理 映射 φ 的象是 SO_3.

证明 我们首先在 SU_2 的对角矩阵的子群 T 上具体算出 $\varphi(P)$. 设 $z=y_3+y_4\mathrm{i}$. 则

【3.17】
$$PAP^*=\begin{bmatrix} a & \\ & \bar{a}\end{bmatrix}\begin{bmatrix} y_2\mathrm{i} & z \\ -\bar{z} & -y_2\mathrm{i}\end{bmatrix}\begin{bmatrix} \bar{a} & \\ & a\end{bmatrix}=\begin{bmatrix} y_2\mathrm{i} & a^2z \\ -\bar{a}^2\bar{z} & -y_2\mathrm{i}\end{bmatrix}.$$

因而 $\varphi(P)$ 保持第一个坐标 y_2 不变并且在 z 上乘以 a^2. 因为 $|a|=1$，故可记 $a=\mathrm{e}^{\mathrm{i}\theta}$. 乘上 $a^2=\mathrm{e}^{\mathrm{i}2\theta}$ 定义了复 z-平面上转过 2θ 的一个旋转. 因而

279

【3.18】
$$\varphi(P)=\begin{bmatrix}1&0&0\\0&\cos2\theta&-\sin2\theta\\0&\sin2\theta&\cos2\theta\end{bmatrix}.$$

这表明 φ 在 SO_3 中的象包含绕点 $(1, 0, 0)^t$ 的所有旋转的子群 H. 这个点对应于矩阵 $E=\begin{bmatrix}\mathrm{i}&\\&-\mathrm{i}\end{bmatrix}$. 由于单位球面 C 是一个共轭类，因此 SU_2 的作用是可迁的. 因此如果 Y 是$\mathbb{R}^3$ 中的任一单位向量，则存在一个元素 $Q\in SU_2$ 使得 $\varphi(Q)(1, 0, 0)^t=Y$，或者用矩阵的记号，有 $QEQ^*=A$. 围绕 Y 的旋转的共轭子群 $\varphi(Q)H\varphi(Q)^*$ 也是 φ 的象. 由于 SO_3 的每个元素都是旋转，故 φ 是满射. ■

上节末提到的构成霍普夫纤维的陪集是 3-球面到 2-球面的连续满射

【3.19】
$$\pi: S^3 \longrightarrow S^2$$

的纤维. 要定义 π，我们像上面一样，将 S^3 解释为特殊酉群 SU_2，而将 S^2 解释为迹零矩阵的共轭类. 令集合 $E=\begin{bmatrix}\mathrm{i}&\\&-\mathrm{i}\end{bmatrix}$，并且对 $P\in SU_2$ 定义 $\pi(P)=PEP^*$. 下列命题的证明留作练习.

280

【3.20】命题 映射 π 的纤维是 SU_2 中对角矩阵群 T 的左陪集 QT.

第四节 特殊线性群 $SL_2(\mathbb{R})$

因为特殊酉群是一个球面，所以它是个紧集. 作为一个非紧群的例子，我们将描述特殊线性群 $SL_2(\mathbb{R})$. 为了简化记号，在本节中用 SL_2 表示 $SL_2(\mathbb{R})$.

可逆 2×2 矩阵以左乘作用在列向量空间$\mathbb{R}^2$ 上，我们可以观察它在$\mathbb{R}^2$ 中射线上的相应的作用. 射线是半直线 $R=\{rX \mid r\geqslant 0\}$. 射线的集合与单位圆 S^1 的点之间有一个一一对应，射线 R 对应于点$R\cap S^1$.

群 SL_2 以左乘作用于射线的集合. 我们用 H 表示 SL_2 中射线 $R_1=\{re_1\}$ 的稳定子. 它由矩阵

【4.1】
$$B=\begin{bmatrix}a&b\\0&a^{-1}\end{bmatrix}$$

组成，其中 a 是正数而 b 为任意数.

旋转群 SO_2 是 SL_2 的另一个子群，它在射线的集合上可迁地作用.

【4.2】命题 由 $f(Q, B)=QB$ 定义的映射 $f: SO_2\times H \longrightarrow SL_2$ 是一个同胚(但不是群同态).

证明 注意 $H\cap SO_2=\{I\}$. 因而 f 是单射[第二章(8.6)]. 要证明 f 是满射，设 P 是 SL_2 的任意元素，并设 R_1 是射线$\{re_1 \mid r\geqslant 0\}$. 选择旋转 $Q\in SO_2$ 使得 $PR_1=QR_1$. 则 $Q^{-1}P$ 属于稳定子 H，比如说 $Q^{-1}P=B$，或者

【4.3】
$$P=QB.$$

由于 f 由矩阵乘法定义，故它是连续映射. 而且在构造逆映射时，因为射线 PR_1 是连续地依赖于 P 的，所以旋转 Q 也是连续地依赖于 P 的. 于是 $B=Q^{-1}P$ 是 P 的连续函数，这证明 f^{-1}

也是连续的. ■

注意 H 可以通过法则 $B\longleftrightarrow(a,b)$ 等同于积空间(正实数)×ℝ. 而通过对数函数，正实数空间同胚于所有实数的空间ℝ. 这样 H 同胚于$\mathbb{R}^2$. 由于 SO_2 是圆，我们得到 [281]

【4.4】$SL_2(\mathbb{R})$同胚于积空间 $S^1\times\mathbb{R}^2$.

用类似于第三节 SU_2 正交表示所用的方法，可以将特殊线性群与二维时空的洛伦兹群 $O_{2,1}$ 联系起来. 设$\mathbb{R}^3$ 的坐标为 y_1，y_2，t，且有洛伦兹型

【4.5】
$$y_1y_1'+y_2y_2'-tt',$$
并设 W 是实的迹零矩阵空间. 利用基

【4.6】
$$\begin{bmatrix}1 & \\ & -1\end{bmatrix},\begin{bmatrix} & 1\\ 1 & \end{bmatrix},\begin{bmatrix} & 1\\ -1 & \end{bmatrix},$$
我们将坐标向量$(y_1,\ y_2,\ t)^t$ 与矩阵

【4.7】
$$A=\begin{bmatrix}y_1 & y_2+t\\ y_2-t & -y_1\end{bmatrix}.$$
联系起来.

我们使用这个迹零矩阵的表示，是因为洛伦兹型(4.5)在这样的矩阵上有一个简单的矩阵解释：

【4.8】
$$\langle A,A'\rangle=y_1y_1'+y_2y_2'-tt'=\frac{1}{2}\text{trace}(AA').$$

群 SL_2 通过共轭在 W 上作用，

【4.9】
$$P,A\rightsquigarrow PAP^{-1},$$
这个作用保持 W 上的洛伦兹型，因为和上一节一样，
$$\text{trace}(AA')=\text{trace}((PAP^{-1})(PA'P^{-1})).$$
由于共轭是 W 上的线性算子，它定义了一个同态 $\varphi:SL_2\longrightarrow GL_3(\mathbb{R})$. 因为共轭保持洛伦兹型，$P$ 的象 $\varphi(P)$是 $O_{2,1}$的一个元素.

【4.10】定理 同态 φ 的核是子群$\{\pm I\}$，而且它的象是 $O_{2,1}$ 中包含单位元 I 的路连通分支 $O_{2,1}^0$. 因而 $O_{2,1}^0\approx SL_2(\mathbb{R})/\{\pm I\}$.

可以证明二维洛伦兹群有四个路连通分支.

φ 的核是$\{\pm I\}$这个事实是容易验证的，定理的最后一个断言可由其他断言推出. 我们略去 φ 的象是子群 $O_{2,1}^0$ 的证明. [282]

第五节 单参数子群

在第四章，我们用级数

【5.1】
$$e^A=I+(1/1!)A+(1/2!)A^2+(1/3!)A^3+\cdots$$
定义矩阵的指数. 现在将用这个函数描述由实数加法群到一般线性群的同态，它是变量 $t\in\mathbb{R}$ 的可微函数. 这样的一个同态称为 GL_n 的单参数子群. (实际上，使用术语"单参数子群"描述这样的同态是名不符实的. φ 的象才应称为子群.)

【5.2】命题

(a) 设 A 是一个任意的实的或复的矩阵，并设 GL_n 根据情形不同而表示 $GL_n(\mathbb{R})$ 或 $GL_n(\mathbb{C})$. 由 $\varphi(t)=e^{tA}$ 定义的映射 $\varphi:\mathbb{R}^+\longrightarrow GL_n$ 是一个群同态.

(b) 反之，设 $\varphi:\mathbb{R}^+\longrightarrow GL_n$ 是一个群同态，它是变量 $t\in\mathbb{R}$ 的可微函数，并用 A 表示在原点处的导数 $\varphi'(0)$. 则对所有 t 有 $\varphi(t)=e^{tA}$.

证明 对任意两个实数 r，s，两个矩阵 rA 和 sA 可交换. 这样第四章(7.13)告诉我们

【5.3】
$$e^{(r+s)A}=e^{rA}e^{sA}.$$

这表明 $\varphi(t)=e^{tA}$ 是一个同态. 反之，设 φ 是一个可微同态 $\mathbb{R}^+\longrightarrow GL_n$. φ 是同态这个假设使得能够计算它在任一点的导数，即有 $\varphi(t+\Delta t)=\varphi(\Delta t)\varphi(t)$ 及 $\varphi(t)=\varphi(0)\varphi(t)$. 这样

【5.4】
$$\frac{\varphi(t+\Delta t)-\varphi(t)}{\Delta t}=\frac{\varphi(\Delta t)-\varphi(0)}{\Delta t}\varphi(t).$$

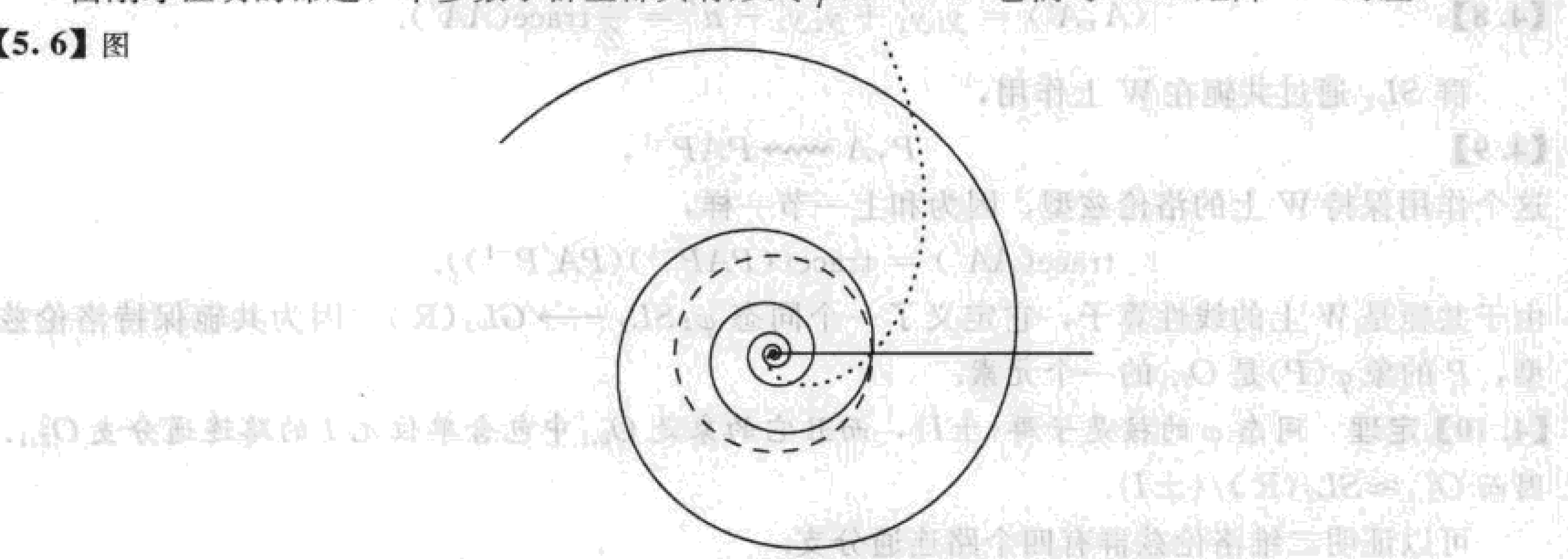
令 $\Delta t\longrightarrow 0$，我们得到 $\varphi'(t)=\varphi'(0)\varphi(t)=A\varphi(t)$. 因而 $\varphi(t)$ 是作为微分方程

【5.5】
$$\frac{d\varphi}{dt}=A\varphi$$

的解的矩阵值函数. 函数 e^{tA} 是另一个解，且在 $t=0$ 处两个解都取值 I. 由此得 $\varphi(t)=e^{tA}$[见第四章(8.14)]. ■

283 由刚才证明的命题，单参数子群全都具有形式 $\varphi(t)=e^{tA}$. 它们与 $n\times n$ 矩阵一一对应.

【5.6】图



$C^\times=GL_1(C)$ 的一些单参数子群

现在假设给定 GL_n 的一个子群 G. 我们要求 G 的单参数子群，也就是同态 $\varphi:\mathbb{R}^+\longrightarrow G$，或等价地说，象属于 G 的到 GL_n 的同态. 因为 GL_n 的单参数子群是由一个矩阵确定的，这相当于求对所有 t 满足 $e^{tA}\in G$ 的矩阵 A. 结果是正维数的线性群总有单参数子群，并且对一个特别的群不难确定它们.

【5.7】例

(a) 复平面上单位圆通常的参数化是 U_1 的一个单参数子群：
$$t \rightsquigarrow e^{ti}=\cos t+i\sin t.$$

(b) 一个相关的例子是在 SO_2 中通过令

$$A=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}\text{得到. 于是 } e^{tA}=\begin{bmatrix}\cos t & -\sin t\\ \sin t & \cos t\end{bmatrix}.$$

这是旋转矩阵的标准参数化.

在例(a)和(b)中，同态的象是整个子群.

(c) 设 A 是 2×2 的矩阵单位 e_{12}. 则由于 $A^2=0$，指数的级数展式中除了两项之外全都为零，并有

$$e^{tA}=I+e_{12}t=\begin{bmatrix}1 & t\\ & 1\end{bmatrix}.$$

这时指数映射定义$\mathbb{R}^+$到其象，也就是对角元素等于 1 的三角矩阵的群的一个同构.

284

(d) SU_2 的单参数子群是对角特殊酉矩阵群的共轭，也就是(2.13)所描述的经.

作为所用方法的例子，我们将对正交和特殊线性群确定单参数子群，而不去试图阐述描述它们的一般定理. 我们需要知道具有逆函数的矩阵的指数函数.

【5.8】命题 矩阵指数将$\mathbb{R}^{n\times n}$中 0 的一个小邻域同胚地映到 I 的一个邻域 T 上.

证明 这个命题由逆函数定理得到，该定理指出如果雅可比矩阵$(\partial f_i/\partial x_j)(p)$可逆，则可微函数 f：$\mathbb{R}^k\longrightarrow\mathbb{R}^k$ 在点 p 有逆函数. 我们必须在$\mathbb{R}^{n\times n}$的零矩阵处对矩阵指数验证这一点. 在记号上这是令人不快的但容易计算. 用 X 表示一个变量矩阵. 雅可比矩阵是其元素为$(\partial(e^X)_{\alpha\beta}/\partial X_{ij})\mid_{X=0}$的 $n^2\times n^2$ 矩阵. 我们运用 $d/dt(e^{tA})\mid_{t=0}=A$ 这一事实. 直接由偏导数的定义可得$(\partial e^X/\partial X_{ij})\mid_{X=0}=(de^{te_{ij}}/dt)\mid_{t=0}=e_{ij}$. 因此 $\alpha,\beta\neq i,j$ 时$(\partial(e^X)_{\alpha\beta}/\partial X_{ij})\mid_{X=0}=0$ 而$(\partial(e^X)_{ij}/\partial X_{ij})\mid_{X=0}=1$. 雅可比矩阵是 $n^2\times n^2$ 恒等矩阵. ■

我们现在描述正交群 O_n 的单参数子群. 这里要求矩阵 A 使得对所有 t 都有 e^{tA} 正交.

【5.9】引理 如果 A 是斜对称的，则 e^A 是正交的. 反过来，存在 0 在$\mathbb{R}^{n\times n}$中的一个邻域 S' 使得若 e^A 正交且 $A\in S'$，则 A 是斜对称的.

证明 为避免将变量 t 与转置矩阵的符号混淆，在这里用 A^* 表示 A 的转置矩阵. 若 A 是斜对称的，则 $e^{(A^*)}=e^{-A}$. 由指数的定义，关系 $e^{(A^*)}=(e^A)^*$ 显然成立，且由第四章(8.10)有 $e^{-A}=(e^A)^{-1}$. 这样$(e^A)^*=e^{(A^*)}=e^{-A}=(e^A)^{-1}$. 这表明 e^A 是正交的. 为证其逆，我们选取 S'充分小使得如果 $A\in S'$，则$-A$ 和 A^* 都在命题(5.8)的邻域 S 之中. 假设 $A\in S'$且 e^A 正交. 则 $e^{(A^*)}=e^{-A}$，而由命题(5.8)，这表明 A 是斜对称的. ■

【5.10】推论 正交群 O_n 的单参数子群是同态 $t\rightsquigarrow e^{tA}$，其中 A 是实的斜对称矩阵.

证明 如果 A 是斜对称的，则对所有 t，tA 也是斜对称的. 从而对所有 t，e^{tA} 是正交的，这表明 e^{tA} 是 O_n 的单参数子群. 反之，假设对所有 t，e^{tA} 是正交的. 对充分小的 ε，εA 属于引理中的邻域 S'并且 $e^{\varepsilon A}$ 正交. 因此 εA 是斜对称的，这也表明 A 也是斜对称的. ■

例(5.7b)对这个推论给予了说明.

285

接下来，我们考虑特殊线性群 $SL_n(\mathbb{R})$.

【5.11】命题 设 A 是迹为零的矩阵. 则 e^A 的行列式为 1. 反之，存在$\mathbb{R}^{n\times n}$中 0 的一个邻域 S'，使得如果 $A\in S'$并且 $\det e^A=1$，则 $\operatorname{trace}A=0$.

证明 第一个断言由一个漂亮的公式得到

【5.12】 $$e^{\mathrm{tr}A} = \det e^A,$$
其中 $\mathrm{tr}A$ 表示矩阵 A 的迹．这个公式又是由下列事实得到的：如果复矩阵 A 的特征值为λ_1，…，λ_n，则 e^A 的特征值为 e^{λ_1}，…，e^{λ_n}．我们将这个事实的证明留作练习．用这个事实，可以得到
$$e^{\mathrm{tr}A} = e^{\lambda_1+\cdots+\lambda_n} = e^{\lambda}_1\cdots e^{\lambda}_n = \det e^A.$$
对于其逆，我们注意到如果 $|x|<1$，则由 $e^x=1$ 得到 $x=0$．选取 S' 足够小，使得如果 $A\in S'$ 则 $\mathrm{tr}A<1$．于是如果 $\det e^A = e^{\mathrm{tr}A}=1$ 并且 $A\in S'$，则 $\mathrm{tr}A=0$． ■

【5.13】**推论** 特殊线性群 $SL_n(\mathbb{R})$ 的单参数子群是同态 $t \rightsquigarrow e^{tA}$，其中 A 是迹为零的实 $n\times n$ 矩阵．

$SL_2(\mathbb{R})$ 的最简单的单参数子群在例(5.7c)中已作了描述．

第六节 李代数

像通常一样，我们将一个线性群 G 视为$\mathbb{R}^{n\times n}$或者$\mathbb{C}^{n\times n}$的子集．在单位矩阵 I 与 G 相切的向量空间称为群的李代数，我们将在本节描述它．

首先回顾切向量的定义．若 $\varphi(t)=(\varphi_1(t), \cdots, \varphi_k(t))$ 是$\mathbb{R}^k$ 中的一条可微路，那么其速度向量 $v=\varphi'(t)$ 是在点 $x=\varphi(t)$ 处路的切向量．这是基本的观察，切向量的概念就由此导出．

假设给定$\mathbb{R}^k$ 的一个子集 S．一个向量 v 称为在点 x 处与 S 相切，如果存在一条完全处于 S 中的可微路 $\varphi(t)$ 使得 $\varphi(0)=x$ 而 $\varphi'(0)=v$．

如果集合 S 是一个或多个多项式函数 $f(x_1, \cdots, x_k)$ 的零点的轨迹，则称之为一个实代数集：

【6.1】 $$S = \{x \mid f(x) = 0\}.$$
例如，$\mathbb{R}^2$ 的单位圆是一个实代数集，因为它是多项式 $f(x_1, x_2)=x_1^2+x_2^2-1=0$ 的零点的轨迹．

286

微分的链式法则给出了一个向量与一个实代数集 S 相切的必要条件．设 $\varphi(t)$ 是 S 中的一条路，并设 $x=\varphi(t)$ 而 $v=\varphi'(t)$．由于路属于 S，所以函数 $f(\varphi(t))$ 恒等于零；因而其导数也恒等于零：

【6.2】 $$0 = \frac{\mathrm{d}}{\mathrm{d}t}f(\varphi(t)) = \frac{\partial f}{\partial x_1}v_1 + \cdots + \frac{\partial f}{\partial x_k}v_k = (\nabla f(x)\cdot v),$$
其中 $\nabla f = \left(\frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_k}\right)$ 是梯度向量．

【6.3】**推论** 设 S 是$\mathbb{R}^k$ 的实代数集，定义为一个或多个多项式函数 $f(x)$ 的零点的轨迹．则 S 在 x 处的切向量与梯度向量 $\nabla f(x)$ 正交．

例如，如果 S 是单位圆而 x 是点(1, 0)，则梯度向量 $\nabla f(0)$ 为(2, 0)．推论(6.3)告诉我们在(1, 0)处的切向量具有$(0, c)$的形式，即它们是互相垂直的向量，事实就是如此．

用参数化路计算切向量的方法是苯拙的，因为许多路有着同样的切线．如果只对切向量感兴趣，则除了其泰勒展开式中的一阶项以外我们可以丢弃一条路所包含的所有信息．为系统地进行处理，我们引入无穷小元素 ε．这是指可以代数地使用法则

【6.4】 $$\varepsilon^2 = 0.$$

正如在复数使用的法则是 $i^2=-1$ 那样，我们可以实系数的在$(1,\varepsilon)$的形式线性组合的向量空间

$$E=\{a+b\varepsilon \mid a,b\in\mathbb{R}\}$$

上用这个法则定义乘法. 乘法的法则是

【6.5】 $$(a+b\varepsilon)(c+d\varepsilon)=ac+(bc+ad)\varepsilon.$$

换言之，利用 $\varepsilon c=c\varepsilon$ 对任意 $c\in\mathbb{R}$ 成立以及 $\varepsilon^2=0$ 这些关系将其形式地展开. 和复数一样，加法是向量加法：

$$(a+b\varepsilon)+(c+d\varepsilon)=(a+c)+(b+d)\varepsilon.$$

$\mathbb{C}$ 和 E 之间主要的区别是 E 不是域，这是因为 ε 没有乘法逆元. [它是一个环(见第十章)].

给定$\mathbb{R}^k$ 的一个点 x 和一个向量 $v\in\mathbb{R}^k$，和 $x+v\varepsilon$ 是一个元素属于 E 的向量，根据直觉我们将其解释为在方向 v 上 x 的无穷小变化. 注意到可用泰勒展开式求多项式 $f(x)=f(x_1,\cdots,x_k)$在 $x+v\varepsilon$ 的取值. 由于 $\varepsilon^2=0$，关于 ε 的次数$\geqslant 2$ 的项都消失了，只剩下 E 中一个元素：

【6.6】 $$f(x+v\varepsilon)=f(x)+\left(\frac{\partial f}{\partial x_1}v_1+\cdots+\frac{\partial f}{\partial x_k}v_k\right)\varepsilon=f(x)+(\nabla f(x)\cdot v)\varepsilon.$$

使用法则(6.4)相当于略去了 ε 的高阶项. 这样点积$(\nabla f(x)\cdot v)$代表当 x 在方向 v 上的无穷小变化时导致的 f 的无穷小变化.

回到由多项式方程 $f(x)=0$ 定义的实代数集 S，设 x 是 S 的点. 则 $f(x)=0$，因而由(6.6)可知

【6.7】 $$f(x+v\varepsilon)=0 \text{ 当且仅当} (\nabla f(x)\cdot v)=0,$$

这与我们在推论(6.3)中得到的条件是相同的. 这令人想到下面的条件：设 S 是由多项式方程 $f(x)=0$ 定义的实代数集. 一个向量 v 称为在 x 处 S 的*无穷小切向量*，如果

【6.8】 $$f(x+v\varepsilon)=0.$$

【6.9】推论 *设 x 是实代数集 S 的点. 每一个 x 处 S 的切向量都是无穷小切向量.*

注意如果固定 $x\in S$，方程$(\nabla f(x)\cdot v)=0$ 是线性的且对于 v 是齐次的. 因而 S 在 x 处的无穷小切向量构成所有向量空间的一个子空间.

实际上，我们的术语有点含混不清. 无穷小切的定义依赖于方程 f，而不仅仅是集合 S. *当说到无穷小切向量的时候，我们必须在心中有特定的方程.*

对于充分光滑的集合 S，(6.9)的逆也成立：每个无穷小切向量都是切向量. 在这种情形下，可以通过关于 v 解线性方程$(\nabla f(x)\cdot v)=0$ 来计算在点 $x\in S$ 处的切向量空间，这相对较为容易. 然而，在集合 S 的"奇异点"，或对于 S 定义的方程选得很糟糕，这个逆就不成立. 例如，设 S 是$\mathbb{R}^2$ 中两个坐标轴的并. 这是由单独一个方程 $x_1x_2=0$ 定义的实代数集合. 显然在原点处切向量必须平行于两个坐标轴之一. 另一方面，$\nabla f=(x_2,x_1)$，当 $x_1=x_2=0$ 时它也为零. 因此每一个向量都是 S 在原点处的一个无穷小切向量.

这就完成了对切向量的一般讨论. 现在将这个讨论应用于当集合 S 是$\mathbb{R}^{n\times n}$或$\mathbb{C}^{n\times n}$中的一个线性群 G 的情形. G 的切向量将是 n^2-维向量，我们仍将用矩阵表示它们. 前面已说过，在单位矩阵 I 处与 G 相切的向量构成群的*李代数*.

要注意的第一点是线性群 G 的每一个单参数子群 e^{tA} 是一条参数化的路. 我们已经知道其

287

速度向量 $\left(\frac{\mathrm{d}e^{tA}}{\mathrm{d}t}\right)_{t=0}$ 是 A. 因而 A 表示在 G 的恒等矩阵处的切向量——它属于李代数. 例如，酉群 U_1 是复平面的单位圆，而 e^{ti} 是 U_1 的单参数子群. 这个单参数子群在 $t=0$ 处的速度向量是向量 i，这的确是单位圆在点 1 处的切向量.

288

一个是 $R^{n\times n}$ 的实代数集的矩阵群 G 称为一个**实代数群**. 如 $SL_n(\mathbb{R})$ 和 O_n 这些典型线性群是实代数群，因为它们的定义方程是其矩阵元素的多项式方程. 例如，群 $SL_2(\mathbb{R})$ 由单独一个多项式方程 $\det P=1$ 定义：

$$x_{11}x_{22}-x_{12}x_{21}-1=0.$$

正交群 O_3 由表达条件 $P^tP=I$ 的九个多项式 f_{ij} 定义：

$$f_{ij}=x_{1i}x_{1j}+x_{2i}x_{2j}+x_{3i}x_{3j}-\delta_{ij}=0,\quad \delta_{ij}=\begin{cases}0, & i\neq j\\ 1, & i=j.\end{cases}$$

像酉群这样的复群也可以在通过将矩阵元素分为其实部和虚部而化成 $\mathbb{R}^{2n\times n}$ 中的实代数群.

有这样一个事实，对实代数群 G 在单位矩阵的每个无穷小切向量 A，e^{tA} 是 G 的单参数子群. 换言之，存在一个单参数子群从单位矩阵指向任意一个切方向上. 对于非阿贝尔群这是非常令人惊讶的，但实质上对它的成立没有什么限制. 遗憾的是，虽然对于特定的群这一事实是容易验证的，但要给出一个一般性的证明则相当困难. 因而我们将满足于对特殊情形的验证.

有了无穷小元素，就可以研究元素属于 E 的矩阵. 这样的矩阵将具有 $A+B\epsilon$ 的形式，其中 A，B 为实矩阵. 从直观上讲，$A+B\epsilon$ 代表 A 的在矩阵 B 方向上的一个无穷小变化. 两个这样矩阵相乘的法则与(6.5)是一样的：

【6.10】 $$(A+B\epsilon)(C+D\epsilon)=AC+(AD+BC)\epsilon.$$

因为对任意指标的取值有 $(b_{ij}\epsilon)(d_{kl}\epsilon)=0$，故乘积 $B\epsilon D\epsilon=0$.

设 G 是一个实代数群. 为求它在单位矩阵的无穷小切向量，必须确定矩阵 A 使得代表 I 的一个在矩阵 A 方向上的无穷小变化的矩阵

【6.11】 $$I+A\epsilon$$

满足定义 G 的方程. 这是无穷小切向量的定义(6.8).

我们对特殊线性群 $SL_n(\mathbb{R})$ 进行这个计算. 这个群的定义方程是 $\det P=1$. 因而如果 $\det(I+A\epsilon)=1$，则 A 是无穷小切向量. 为描述这一条件，必须计算当在 I 上作一个无穷小变化时行列式的变化. 公式是漂亮的：

【6.12】 $$\det(I+A\epsilon)=1+(\operatorname{trace}A)\epsilon.$$

289

这个公式的证明留作练习. 使用这个公式，可以得到 A 是无穷小切向量当且仅当 $\operatorname{trace}A=0$.

【6.13】命题 *对于实 $n\times n$ 矩阵 A 下列条件等价：*

(i) $\operatorname{trace}A=0$；

(ii) e^{tA} 是 $SL_n(\mathbb{R})$ 的单参数子群；

(iii) A 属于 $SL_n(\mathbb{R})$ 的李代数；

(iv) A 是 $SL_n(\mathbb{R})$ 在 I 处的无穷小切向量.

证明 命题(5.11)告诉我们(i)⇒(ii). 由于 A 在 $t=0$ 与路 e^{tA} 相切，故(ii)⇒(iii). 蕴涵关系(iii)⇒(iv)是(6.9)，而(iv)⇒(i)由(6.12)得到. ■

这里有一个一般的原则．我们有矩阵 A 的三个集合：使 e^{tA} 是 G 的单参数子群的那些矩阵，属于李代数的那些矩阵以及本身是无穷小切向量的那些矩阵．我们用 $\mathrm{Exp}(G)$，$\mathrm{Lie}(G)$ 和 $\mathrm{Inf}(G)$ 表示这三个集合．它们由下列包含关系联系起来：

【6.14】
$$\mathrm{Exp}(G) \subset \mathrm{Lie}(G) \subset \mathrm{Inf}(G).$$

因为 A 是 e^{tA} 在 $t=0$ 处的切向量，第一个包含关系成立；因为每个切向量是一个无穷小切向量，第二个包含关系成立．如果 $\mathrm{Exp}(G)=\mathrm{Inf}(G)$，则这两个集合都等于 $\mathrm{Lie}(G)$．因为 $\mathrm{Exp}(G)$ 和 $\mathrm{Inf}(G)$ 容易计算，这给出了一个求李代数的实用的方法．如果恰当地选择其定义方程，则有一个一般的定理，它蕴涵对每个实代数群有 $\mathrm{Exp}(G)=\mathrm{Inf}(G)$．但在这里证明这个一般定理是不值得的．

我们现在对正交群 O_n 进行计算．O_n 的定义方程是矩阵方程 $P^tP=I$．为使 A 成为在单位矩阵的无穷小切向量，它必须满足关系

【6.15】
$$(I+A\varepsilon)^t(I+A\varepsilon) = I.$$

关系式左边展开为 $I+(A^t+A)\varepsilon$，因此 $(I+A\varepsilon)$ 正交的条件是 $A^t+A=0$，或 A 是斜对称的．这与 e^{tA} 是 O_n 的单参数子群的条件(5.10)是一致的．

【6.16】命题 对于实 $n\times n$ 矩阵 A 下列条件等价：

(i) A 是斜对称的；

(ii) e^{tA} 是 O_n 的单参数子群；

(iii) A 属于 O_n 的李代数；

(iv) A 是 O_n 在 I 的无穷小切向量．

线性群的李代数还有另一个结构，称为李括号的运算．李括号是由法则

【6.17】
$$[A,B] = AB - BA$$

定义的合成法则．这个合成法则不是结合的．然而，它却满足称为雅可比恒等式的恒等式，

【6.18】
$$[A,[B,C]] + [B,[C,A]] + [C,[A,B]] = 0,$$

它代替了结合律．

为证括号是李代数的合成法则，必须验证如果 A，B 属于 $\mathrm{Lie}(G)$，则 $[A, B]$ 也属于 $\mathrm{Lie}(G)$．对任意特定的群，这都是容易验证的．对于特殊线性群，需要验证的是如果 A，B 的迹为零，则 $AB-BA$ 的迹也为零．因为 $\mathrm{trace}AB=\mathrm{trace}BA$，所以这是成立的．而当 $G=O_n$ 时，李代数是斜对称矩阵空间．我们必须验证如果 A，B 是斜对称的，则 $[A, B]$ 也是：

$$[A,B]^t = (AB-BA)^t = B^tA^t - A^tB^t = BA - AB = -[A,B],$$

这正是所要证的．

括号运算的重要性在于它是换位子 $PQP^{-1}Q^{-1}$ 的无穷小版本．要看到这一点，需要用到两个无穷小量 ε，δ，使用法则 $\varepsilon^2=\delta^2=0$ 和 $\varepsilon\delta=\delta\varepsilon$．注意到矩阵 $I+A\varepsilon$ 的逆是 $I-A\varepsilon$．于是如果 $P=I+A\varepsilon$ 而 $Q=I+B\delta$，则换位子展开成为：

【6.19】
$$(I+A\varepsilon)(I+B\delta)(I-A\varepsilon)(I-B\delta) = I + (AB-BA)\varepsilon\delta.$$

直观上看，括号运算的结果属于李代数，这是因为两个 G 中的元素甚至是两个无穷小元素的乘积仍属于 G，因而两个元素的换位子也在 G 中．

利用括号运算，也可以抽象地定义李代数的概念．

【6.20】定义 域 F 上的李代数 V 是一个向量空间，具有称为括号的合成法则

$$V\times V\longrightarrow V$$
$$v,w \rightsquigarrow [v,w],$$

具有性质：对所有 u，v，$w\in V$ 及所有 $c\in F$，有

(i) 双线性性：

$$[v_1+v_2,w]=[v_1,w]+[v_2,w],\quad [cv,w]=c[v,w],$$
$$[v,w_1+w_2]=[v,w_1]+[v,w_2],\quad [v,cw]=c[v,w],$$

(ii) 斜对称：$[v,\ v]=0$，

(iii) 雅可比恒等式：$[u,\ [v,\ w]]+[v,\ [w,\ u]]+[w,\ [u,\ v]]=0$.

李代数的重要性来自下列事实：作为向量空间，它们与线性群自身相比处理起来要容易得多，同时典型群差不多是由它们的李代数确定的．换句话说，群在单位元处的无穷小结构几乎足以确定群．

291

第七节 群的平移

本节中将用到另一个拓扑概念——$\mathbb{R}^k$ 中流形的定义．在附录中复习了这个定义[定义(3.12)]．如果对流形的概念不熟也不必泄气．随着学习的深入，将不会有太大的麻烦就能学到所必需的东西．

设 P 是矩阵群 G 的一个固定元素．我们知道用 P 左乘是从 G 到自身的一个双射：

【7.1】

$$G\xrightarrow{m_P}G$$
$$X\rightsquigarrow PX,$$

这是因为它有逆函数 $m_{P^{-1}}$．映射 m_P 和 $m_{P^{-1}}$ 都是连续的，这是因为矩阵乘法是连续的．这样 m_P 是 G 到自身的同胚(不是同态)．它亦称为由 P 给出的*左平移*，这类似于平面上的平移，也就是加法群 $\mathbb{R}^{2+}$ 的左平移．

这些映射的存在性蕴涵的群的一个重要性质是齐性．用 P 左乘是将恒等元素 I 映到 P 的一个同胚．因而群 G 在 I 附近的拓扑结构与在 P 附近的拓扑结构是一样的，而由于 P 是任意的，因而在群中任意两点的邻域是相同的．这类似于平面上在任意两点看起来都是一样的这个事实．

SU_2 中的左乘恰好由一个坐标 $(x_1,\ x_2,\ x_3,\ x_4)$ 的正交变换定义，因而它是 3-球面的一个刚体运动．但用一个矩阵左乘不一定是刚体运动，只有在较弱的意义下才能使任意群都是齐次的．例如，设 G 是实 2×2 逆对角矩阵的群，并且将 G 的元素与平面上不在坐标轴上的点 $(a,\ d)$ 等同起来．用矩阵

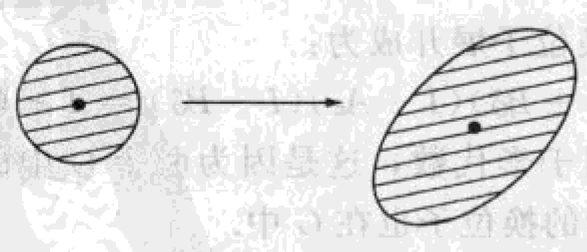
【7.2】

$$P=\begin{bmatrix}2&0\\0&1\end{bmatrix}$$

左乘使群 G 变形，但这种变形是连续的．

【7.3】图

292



一个群中的左乘

$\mathbb{R}^k$ 中在几何上具有这样的齐性的合情合理的子集只有流形. 一个 d 维流形 M 是在其每个点都局部地同胚于$\mathbb{R}^d$ 的子集，这是指每个点 $p\in M$ 有一个邻域同胚于$\mathbb{R}^d$ 的一个开集[见附录(3.12)]. 由于具有齐性，典型群是流形并不使人感到意外，虽然 GL_n 有的子群不是流形. 例如，有理系数的可逆矩阵的群 $GL_n(\mathbb{Q})$虽然是一个很有意思的群，但从几何上看它是非常糟糕的. 下面的定理对哪些线性群是流形这个问题给出了一个令人满意的回答.

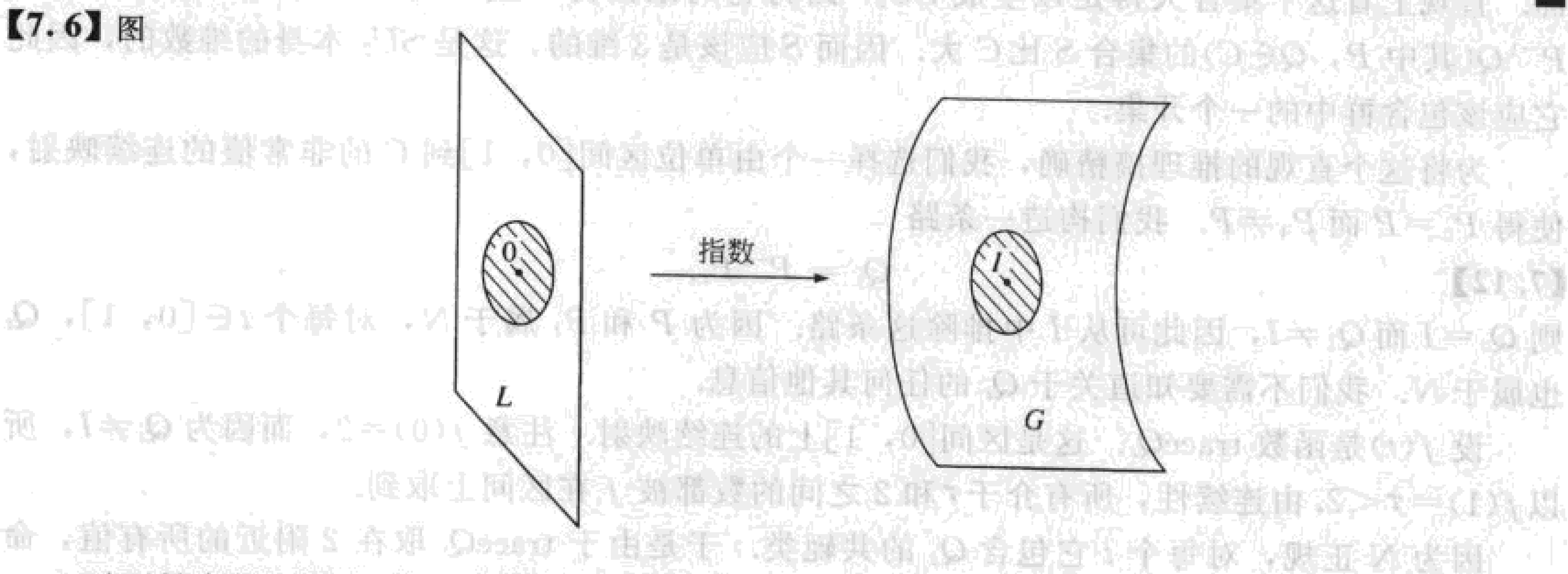
【7.4】定理 设 G 是 $GL_n(\mathbb{R})$的在$\mathbb{R}^{n\times n}$中是闭集的子群. 则 G 是流形.

在这里给出这个定理的证明将把我们带离主题太远. 我们转而通过证明正交群 O_n 是流形来说明这个定理. 对其他典型群的证明是类似的.

【7.5】命题 正交群 O_n 是$\frac{1}{2}n(n-1)$维流形.

证明 用 G 表示 O_n 而用 L 表示其李代数，也就是斜对称矩阵的空间. 命题(5.9)告诉我们对于在 0 附近的矩阵 A，有 $A\in L$ 当且仅当 $e^A\in G$. 而且指数是由$\mathbb{R}^{n\times n}$中 0 的一个邻域到 I 的一个邻域的同胚. 把这两个事实放到一起，我们发现指数定义了 L 中 0 的邻域到 G 中 I 的邻域的一个同胚. 由于 L 是一个$\frac{1}{2}n(n-1)$维空间，故它是一个流形. 这表明正交群在单位矩阵处满足成为流形的条件. 另一方面，我们在上面看到 G 中任意两点具有同胚的邻域. 因此正如所断言的，G 是一个流形. ■

【7.6】图



下面是齐性原则的另一个应用.

【7.7】命题 设 G 是路连通矩阵群，并设 $H\subset G$ 是包含 G 的一个非空开集的子群. 则 $H=G$.

证明 由假设，H 包含 G 的一个非空开集 U. 由于用 $g\in G$ 左乘是一个同胚，故 gU 也是 G 中的开集. 每个平移 gU 包含在 H 的一个单独的陪集中，即在 gH 中，因为 U 的平移覆盖了 G，它们也覆盖了每个陪集. 这样，每个陪集是 G 的开子集的并，因而它本身也是开的. 因而 G 划分为开子集——也就是 H 的陪集. 而路连通集不是其真开子集的不相交并[见附录，命题(3.11)]. 这样就只能有一个陪集，即 $H=G$. ■

我们将用这个命题确定 SU_2 的正规子群.

【7.8】定理 SU_2 的真的正规子群只有其中心$\{\pm I\}$.

由于存在一个满射 $\varphi: SU_2 \longrightarrow SO_3$，其核为$\{\pm I\}$，因此旋转群同构于 SU_2 的商群[第

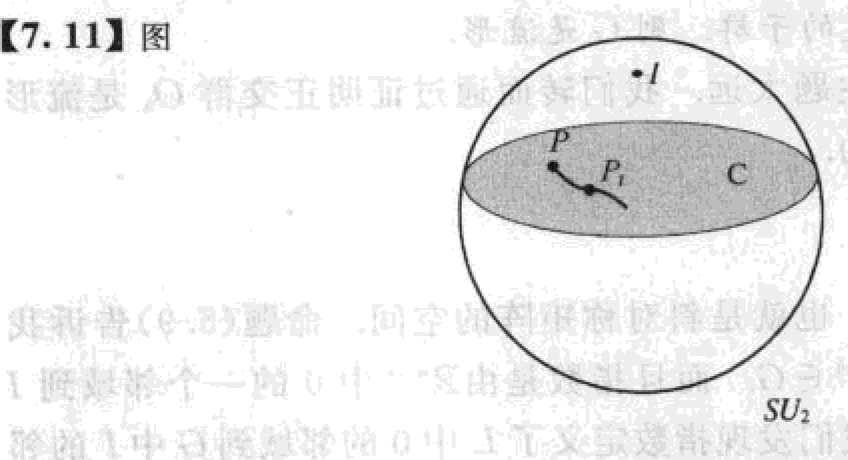
二章(10.9)]：

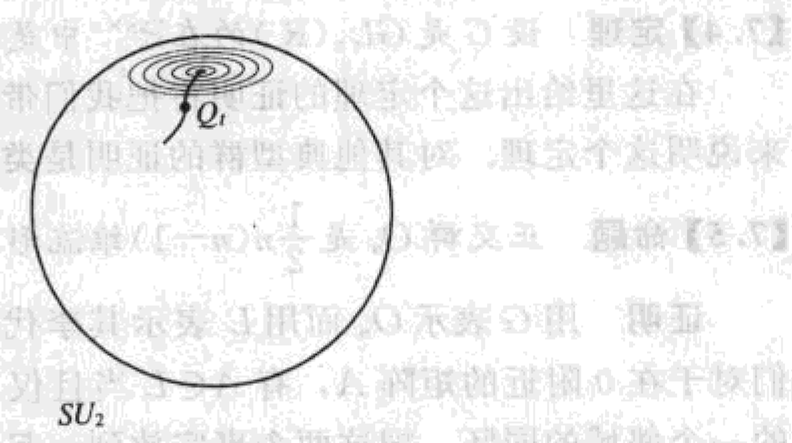
【7.9】 $$SO_3 \approx SU_2/\{\pm I\}.$$

【7.10】推论 SO_3 是单群，即它没有真的正规子群.

证明 SO_3 中正规子群的原象是 SU_2 中包含$\{\pm I\}$的正规子群[第二章(7.4)]. 定理(7.8)告诉我们它没有真的正规子群. ■

【7.11】图





294

定理(7.8)的证明 只需证明如果 N 是不含于中心$\{\pm I\}$的正规子群，则 N 是整个群. 既然 N 是正规的，它是共轭类的并[第六章(2.5)]. 我们已看到共轭类是纬，即 2-球面(2.8). 由假设，N 包含一个矩阵 $P\neq\pm I$，因而它包含整个共轭类 $C=C_P$，而这个共轭类是一个 2-球面. 直观上看这个集合大得足以生成 SU_2. 因为它的维数为 2 且不是个子群. 因而所有乘积 $P^{-1}Q$(其中 P，$Q\in C$)的集合 S 比 C 大. 因而 S 应该是 3 维的，这是 SU_2 本身的维数的，因此它应该包含群中的一个开集.

为将这个直观的推理搞精确，我们选择一个由单位区间[0，1]到 C 的非常值的连续映射，使得 $P_0=P$ 而 $P_1\neq P$. 我们构造一条路

【7.12】 $$Q_t = P^{-1}P_t.$$

则 $Q_0=I$ 而 $Q_1\neq I$，因此可从 I 中排除这条路. 因为 P 和 P_t 属于 N，对每个 $t\in[0，1]$，Q_t 也属于 N. 我们不需要知道关于 Q_t 的任何其他信息.

设 $f(t)$是函数 traceQ_t. 这是区间[0，1]上的连续映射. 注意 $f(0)=2$，而因为 $Q_t\neq I$，所以$f(1)=\tau<2$. 由连续性，所有介于τ和 2 之间的数都被 f 在区间上取到.

因为 N 正规，对每个 t 它包含 Q_t 的共轭类. 于是由于 traceQ_t 取在 2 附近的所有值，命题(2.9)告诉我们 N 包含 SU_2 中迹充分靠近 2 的所有矩阵，这就包含了所有充分靠近 I 的矩阵. 因而 N 包含 I 在 SU_2 中的一个开邻域. 现在由于 SU_2 是球面，它是路连通的，因而用命题(7.7)就完成了证明. ■

也可以把群的平移应用于切向量. 如果 A 是在单位矩阵的切向量，并且如果 $P\in G$ 是任意的，则 PA 是在点 P 与 G 相切的向量. 直观上讲，这是因为 $P(I+A\epsilon)=P+PA\epsilon$ 是 G 中元素的乘积，因而它本身属于 G. 与通常一样，这一事实对特定的群是容易验证的. 固定 A，将切向量 PA 与 G 的元素 P 相联系. 用这种方法我们得到群 G 的*切向量场*. 由于 A 是非零的而 P 是可逆的，这个向量场在任何点都不会消失. 仅是存在无处为零的切向量场这一点就对空间 G 加上了很强的条件. 例如，拓扑学的一个定理指出 2-球面上任意向量场必在某个点为零. 这就是为什么 2-球面没有群结构的原因. 但作为群的 3-球面具有无处为零的切向量场.

第八节 单 群

回顾一个群 G 称为单的，如果它不是平凡群并且不包含真的正规子群(第六章第二节)．迄今为止，我们已见到两个非阿贝尔单群：二十面体群 $I\approx A_5$［第六章(2.3)］和旋转群 SO_3 (7.10)．本节讨论单群的分类．我们将省去大部分证明．

单群重要的原因有两个．首先，如果一个群 G 有真正规子群 N，则知道了 N 与商群 G/N 的结构时，也部分地刻画了 G 的结构．如果 N 或 G/N 有正规子群，则可进一步分解这些群的结构．以这种方式我们希望通过从单群归纳地将它构造出来而刻画给定的有限群． 295

其次，虽然单群这个条件是个很强的限制，单群还是常常出现．典型线性群就几乎是单的．例如，上节我们看到 SU_2 的中心为$\{\pm 1\}$且 $SU_2/\{\pm 1\}\approx SO_3$ 是个单群．其他典型群有类似的性质．

为集中注意力，我们在这里将讨论限于复群．用符号 Z 表示任意群的中心．下面的定理的证明会化太多的时间，但我们将对 $SL_2(\mathbb{C})$这一特殊情形加以说明．

【8.1】定理

(a) 特殊线性群 $SL_n(\mathbb{C})$的中心 Z 是一个循环群，由矩阵 ζI 生成，其中 $\zeta=e^{\frac{2\pi i}{n}}$．当 $n\geqslant 2$ 时商群 $SL_n(\mathbb{C})/Z$ 是单群．

(b) 如果 n 是偶数，复特殊正交群 $SO_n(\mathbb{C})$的中心 Z 是$\{\pm I\}$；如果 n 是奇数，其中心是平凡群$\{I\}$．如果 $n=3$ 或 $n\geqslant 5$，群 $SO_n(\mathbb{C})/Z$ 是单群．

(c) 辛群 $SP_{2n}(\mathbb{C})$的中心 Z 是$\{\pm I\}$，并且如果 $n\geqslant 1$，$SP_{2n}(\mathbb{C})/Z$ 是单群． ■

群 $SL_n(\mathbb{C})/Z$ 称为射影群并记为 $PSL_n(\mathbb{C})$：

【8.2】 $$PSL_n(\mathbb{C}) = SL_n(\mathbb{C})/Z,\quad 其中\ Z=\{\zeta I \mid \zeta^n = 1\}.$$

为说明定理(8.1)，我们将证明 $PSL_2(\mathbb{C})=SL_2(\mathbb{C})/\{\pm I\}$是单群．事实上，将证明对几乎所有域 F，$PSL_2(\mathbb{C})$是单群．

【8.3】定理 设 F 是特征不为2的域并且至少含有七个元素．则 $SL_2(F)$仅有的真正规子群为$\{\pm I\}$．因此 $PSL_2(F)=SL_2(F)/\{\pm I\}$是单群．

由于 $SL_2(F)$的中心是正规子群，由定理得到它是群$\{\pm I\}$．

【8.4】推论 存在无穷多个非阿贝尔的有限单群．

定理(8.3)的证明 证明是代数的，但它与上节给出的 SU_2 的类似断言的几何证明是密切相关的．我们的方法是作共轭和乘积直到群被生成．为简化记号，用 SL_2 表示 $SL_2(F)$．设 N 是 SL_2 的正规子群，它包含一个矩阵 $A\neq\pm I$．我们要证 $N=SL_2$．因为一种可能性是 N 是由 A 及其共轭生成的正规子群，所以必须证这个矩阵的共轭足以生成整个群． 296

证明的第一步是证明 N 中包含一个不是$\pm I$ 的三角矩阵．如果给定的矩阵 A 的特征值属于F，则它将共轭于一个三角矩阵．但由于我们想考虑任意域，这一步就不是那么容易了．虽然对于复数这一步是容易的，但对一般域它是最难的一部分证明．

【8.5】引理 N 包含一个三角矩阵 $A\neq\pm I$．

证明 设 $A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$是 N 中一个不是 $\pm I$ 的矩阵. 若 $c=0$，则 A 是所需的矩阵.

假设 $c\neq 0$. 在这一情形，我们将用 A 及其共轭构造一个三角矩阵. 首先计算共轭

$$\begin{bmatrix}1 & x\\ & 1\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & -x\\ & 1\end{bmatrix}=\begin{bmatrix}a+xc & *\\ c & d-xc\end{bmatrix}=A'.$$

由于 $c\neq 0$，可取 x 使 $a+xc=0$. 矩阵 A'属于 N，因而 N 包含一个左上角元素为零的矩阵. 用这个矩阵代替 A，使之具有形式 $A=\begin{bmatrix} & b\\ c & d\end{bmatrix}$. 遗憾的是零的位置不对.

注意由于 $\det A=1$，在我们的新矩阵中有 $bc=-1$. 现在计算它与一个对角矩阵的换位子 $P^{-1}A^{-1}PA$：

$$P^{-1}A^{-1}PA=\begin{bmatrix}u & \\ & u^{-1}\end{bmatrix}\begin{bmatrix}d & -b\\ -c & \end{bmatrix}\begin{bmatrix}u^{-1} & \\ & u\end{bmatrix}\begin{bmatrix} & b\\ c & d\end{bmatrix}=\begin{bmatrix}u^2 & (1-u^2)bd\\ & u^{-2}\end{bmatrix}.$$

这个矩阵属于正规子群 N，只要它不是 $\pm I$ 就是所需要的矩阵. 如果它是 $\pm I$，则 $u^2=\pm 1$ 且 $u^4=1$. 但我们可自由地使用任意一个 $F^\times$ 中的元素 u 构造矩阵 P. 我们将证明[第十一章(1.8)]多项式 x^4-1 在任意域中最多有四个根. 因而最多有四个元素 $u\in F^\times$ 使得 $u^4=1$. 我们的假设是 $F^\times$ 至少含有五个元素. 因而可选择 $u\in F^\times$ 且 $u^4\neq 1$. 于是 $P^{-1}A^{-1}PA$ 是所求的矩阵. ■

【8.6】引理 N 含有一个形如$\begin{bmatrix}1 & u\\ & 1\end{bmatrix}$的矩阵，且 $u\neq 0$.

证明 由前面的引理，N 包含一个三角矩阵 $A=\begin{bmatrix}a & b\\ & d\end{bmatrix}\neq\pm I$. 如果 $d\neq a$，设 $A'=\begin{bmatrix}a & b'\\ & d\end{bmatrix}$为它在矩阵$\begin{bmatrix}1 & 1\\ & 1\end{bmatrix}$下的共轭. 则 $b'=b+d-a$. 由于 $\det A=ad=1$，积

$$A'^{-1}A=\begin{bmatrix}d & -b'\\ & a\end{bmatrix}\begin{bmatrix}a & b\\ & d\end{bmatrix}=\begin{bmatrix}1 & ad-d^2\\ & 1\end{bmatrix}$$

297

是所求的矩阵. 如果 $a=d$，则因为 $\det A=1$，故 $a=\pm 1$，并且由此得到 $b\neq 0$. 在这种情形中，两个矩阵 A 或 A^2 中的一个即为所求. ■

【8.7】引理 设 F 是域. 对所有 $a\neq 0$，矩阵$\begin{bmatrix}1 & u\\ & 1\end{bmatrix}$在 SL_2 中的共轭类包含矩阵$\begin{bmatrix}1 & \\ -u & 1\end{bmatrix}$和$\begin{bmatrix}1 & a^2u\\ & 1\end{bmatrix}$.

证明

$$\begin{bmatrix} & -1\\ 1 & \end{bmatrix}\begin{bmatrix}1 & u\\ & 1\end{bmatrix}\begin{bmatrix} & 1\\ -1 & \end{bmatrix}=\begin{bmatrix}1 & \\ -u & 1\end{bmatrix},\quad\begin{bmatrix}a & \\ & a^{-1}\end{bmatrix}\begin{bmatrix}1 & u\\ & 1\end{bmatrix}\begin{bmatrix}a^{-1} & \\ & a\end{bmatrix}=\begin{bmatrix}1 & a^2u\\ & 1\end{bmatrix}.$$ ■

【8.8】引理 设 F 是特征$\neq 2$ 的域. 域的加法群 F^+ 由 F 的元素的平方生成.

证明 我们证明每个元素 $x\in F$ 可以写成 $a^2-b^2=(a+b)(a-b)$的形式，其中 a，$b\in F$. 为此解线性方程组 $a+b=1$，$a-b=x$. 这就是使用 F 的特征不是 2 这一假设的地方. 在特征

为 2 的情形下，这些方程不一定有解. ■

【8.9】引理 设 F 是特征 $\neq 2$ 的域. 如果 $SL_2(F)$ 的正规子群 N 包含一个满足 $u\neq 0$ 的矩阵 $\begin{bmatrix}1 & u\\ & 1\end{bmatrix}$，则它包含了所有这样的矩阵.

证明 满足 $\begin{bmatrix}1 & x\\ & 1\end{bmatrix}\in N$ 的 x 的集合是 F^+ 的一个子群，称之为 S. 我们想要证明 $S=F^+$. 引理(8.7)表明如果 $u\in S$，则对所有 $a\in F$ 有 $a^2u\in S$. 由于平方生成 F^+，元素的集合 $\{a^2u\mid a\in F\}$ 生成 F^+ 的加法子群 F^+u，并且因为 u 是可逆的，这个子群等于 F^+. 这样正如所需要的，有 $S=F^+$. ■

【8.10】引理 对每个域 F，群 $SL_2(F)$ 由初等矩阵 $\begin{bmatrix}1 & u\\ & 1\end{bmatrix}$ 和 $\begin{bmatrix}1 & \\ u & 1\end{bmatrix}$ 生成.

证明 对矩阵 $A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\in SL_2(F)$ 做行约化，只用这个形式的矩阵. 从第一列开始，将它约化成 e_1. 必要时将第一行加到第二行上，从而排除 $c=0$ 的情形. 然后将第二行的一个倍数加到第一行将 a 变为 1. 最后消去元 c. 至此，矩阵具有形式 $A'=\begin{bmatrix}1 & b'\\ 0 & d'\end{bmatrix}$. 则 $d'=\det A'=\det A=1$，于是可以消去元素 b'，最终得到单位矩阵. 因为需要四个或更少的变换将其化为单位矩阵，所以 A 最多是四个这样的初等矩阵的乘积. ■

298

将引理(8.6)、(8.7)、(8.9)和(8.10)组合起来就完成了定理(8.3)的证明. ■

嘉当的一个著名定理断言(8.1)所列出的几乎就是全部单群了. 当然还有别的单群，例如，我们刚才证明对大多数域 F，$PSL_2(F)$是单群. 但如果限制到复代数群，则单群的列表会变得很短.

$GL_n(\mathbb{C})$ 的子群 G 称为一个**复代数群**，如果它是有限多个矩阵元素的多项式方程组的解的集合. 这与第六节所引入的实代数群的概念类似. 为什么由多项式方程组定义性质是个合理的条件并不显然，但有一点是容易看出的：除了酉群 U_n 及 SU_n，所有复典型群是复代数群.

【8.11】定理

(a) 群 $PSL_n(\mathbb{C})=SL_n(\mathbb{C})/Z$，$SO_n(\mathbb{C})/Z$ 及 $SP_{2n}(\mathbb{C})/Z$ 是路连通的复代数群.

(b) 除了这些群的同构类，恰好存在五个单的路连通复代数群的同构类，称之为例外群.

定理(8.11)太难而无法在这里证明. 它基于对应的李代数的一个分类. 我们所应该知道的是没有多少单代数群. 这应该在最后一章之后重新得到确认，那里在一个接一个的向量空间上引入一个又一个结构，每个都有其自己的对称群. 这似乎无穷无尽. 现在我们看到实际上遇到了大多数可能的对称的类型，至少是那些与单代数群相联系的. 这些结构是重要的这一点并不是偶然的.

有限单群的分类这样一个大的课题在 1980 年完成. 我们看到的有限单群有素数阶群、二十面体群 $I\approx A_5$[第六章(2.3)]以及 F 是有限域时的群 $PSL_2(F)$(8.3)，但还有许多. 对所有 $n\geqslant 5$，交错群 A_n 是单群.

线性群在有限单群以及复代数群的分类中起着决定性的作用. 当用有限域代替复数域时，

形如(8.11)的每一个单群都给出一整个系列的有限单群. 还有一些有限单群与西群类似. 所有这些有限线性群称之为**李型群**.

根据定理(8.3), $PSL_2(\mathbb{F}_7)$是有限单群, 其阶为 168. 这是第二小的非阿贝尔单群; A_5 是最小的. 一些最小的非阿贝尔单群的阶是

299 **【8.12】** $$60, 168, 360, 504, 660, 1092, 2448.$$

对这七个整数中的每一个 N, 有单独一个 N 阶单群的同构类, 且它由某个适当的有限域 F 上的 $PSL_2(F)$表示. [交错群 A_5 碰巧同构于 $PSL_2(\mathbb{F}_5)$.]

除了素数阶群、交错群及李型群, 还有恰好 26 个有限单群称为**零散群**. 最小的零散群是马休群 M_{11}, 其阶为 7920. 最大的称为**大魔群**; 其阶大约是 10^{53}. 因而有限单群形成一个列表, 它虽然要更长些, 但在某种程度上仍类似于单代数群的列表(8.11).

簇拥在成功的理论周围而将其失败扫除门外似乎是不公平的.

Richard Brauer

练 习

第一节 典型线性群

1. (a) 求 $GL_2(\mathbb{R})$中一个与$\mathbb{C}^\times$同构的子群.
   (b) 证明对每一个 n, $GL_n(\mathbb{C})$同构于 $GL_{2n}(\mathbb{R})$的一个子群.
2. 证明 $SO_2(\mathbb{C})$不是$\mathbb{C}^4$ 的一个有界集.
3. 证明 $SP_2(\mathbb{R})=SL_2(\mathbb{R})$, 但是 $SP_4(\mathbb{R})\neq SL_4(\mathbb{R})$.
4. 根据西尔维斯特法则, 每个 2×2 实对称矩阵恰与六个标准类型之一相合. 将它们列出来. 如果考虑 $GL_2(\mathbb{R})$ 通过 $P, A \rightsquigarrow PAP^t$ 在 2×2 矩阵上的作用, 则西尔维斯特法则断言对称矩阵构成六条轨道. 我们可将对称矩阵视为$\mathbb{R}^3$ 中的点, 设(x, y, z)对应于矩阵$\begin{bmatrix} x & y \\ y & z \end{bmatrix}$. 将$\mathbb{R}^3$ 具体分解为轨道, 并清楚地作图来显示得到的几何结构.
5. 矩阵 P 是正交的当且仅当其列构成一个标准正交基. 刻画为使矩阵属于洛伦兹群 $O_{3,1}$ 而其列必须具有的性质.
6. 证明不存在正交群 O_4 到洛伦兹群 $O_{3,1}$ 的连续同构.
7. 用方程描述 $O_{1,1}$, 并证明它具有四个连通分支.
8. 描述 $SL_2(\mathbb{R})$通过 $P, A \rightsquigarrow PAP^t$ 在实对称矩阵空间上作用的轨道.
9. 设 F 是特征不为 2 的域. 描述 $GL_2(F)$在系数属于 F 的 2×2 对称矩阵空间上的作用 $P, A \rightsquigarrow PAP^t$ 的轨道.
10. 设 $F=\mathbb{F}_2$. 通过求每一个相合类的代表对 $GL_n(F)$在 $n\times n$ 对称矩阵空间上作用的轨道进行分类. 300
11. 证明下列矩阵是辛的, 如果其块为 $n\times n$ 的: $\begin{bmatrix} & -I \\ I & \end{bmatrix}$, $\begin{bmatrix} A^t & \\ & A^{-1} \end{bmatrix}$, $\begin{bmatrix} I & B \\ & I \end{bmatrix}$, 其中 $B=B^t$ 而 A 可逆.
12. 证明辛群 $SP_{2n}(\mathbb{R})$在$\mathbb{R}^{2n}$上可迁地作用.

*13. 证明 $SP_{2n}(\mathbb{R})$是路连通的, 并由此得出每个辛矩阵的行列式为 1.

第二节 特殊酉群 SU_2

1. 设 P，Q 是由实向量(x_1, x_2, x_3, x_4)，(y_1, y_2, y_3, y_4)表示的 SU_2 的元素．计算对应于乘积 PQ 的实向量．
2. 证明 SU_2 的子群 SO_2 与对角矩阵的子群 T 共轭．
3. 证明 SU_2 是路连通的．对 SO_3 作同样的证明．
4. 证明 U_2 与积 $S^3 \times S^1$ 同胚．
5. 设 G 是形如$\begin{bmatrix} x & y \\ & 1 \end{bmatrix}$的矩阵的群，其中 x，$y \in \mathbb{R}$ 且 $x>0$．确定 G 中的共轭类并将它们在(x, y)-平面上画出来．

*6. (a) 证明 SU_2 的每个元素 P(2.4)可以写为乘积 $P=DRD'$，其中 D，$D' \in T$(2.13)，且 $R \in SO_2$ 是一个转过角度 $\theta(0 \leqslant \theta \leqslant \pi/2)$的旋转．
   (b) 假设 P 的矩阵元素 a，b 是非零的．证明除了对 D，D'可以用$-D$，$-D'$代替以外，这个表示是唯一的．
   (c) 描述双陪集 TPT，$P \in SU_2$．证明如果 P 的矩阵元素 a，b 是非零的，则双陪集同胚于环面，并描述剩下的双陪集．

第三节 SU_2 的正交表示

1. 对 SU_2 的共轭作用计算矩阵$\begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$的稳定子 H，并对 $P \in H$ 描述 $\varphi(P)$．
2. 证明 SU_2 的每一个大圆是经(2.14)之一中的一个陪集．
3. 求同胚于空间 $S \times \Theta$(3.4)的$\mathbb{R}^3$ 的子集．
4. 推导一个用 A 的行列式表出$\langle A, A\rangle$的公式．
5. 通过将矩阵映到其第一列可将旋转群 SO_3 映到 2-球面．描述这个映射的纤维．
6. 将本节定义的映射 φ 拓广为同态 Φ：$U_2 \longrightarrow SO_3$，并描述 Φ 的核．
7. 通过直接计算证明矩阵(3.11)属于 SO_3．

*8. 仔细描述 SO_3 中的共轭类，并将它们与 SU_2 中的共轭类联系起来．

9. 证明 SU_2 在除去$\{I\}$和$\{-I\}$外的共轭类上的作用由球面的旋转给出．
10. 求一个 SO_3 中的元素与由单位 2-球面上的点 p 与在 p 点处与 S 相切的单位切向量 v 组成的对(p, v)之间的一一对应．
11. 证明命题(3.20)．

*12. (a) 用坐标 x_1，x_2，x_3，x_4 具体算出用固定矩阵 P 在 SU_2 的左乘．证明它是用 4×4 正交矩阵 Q 的左乘，因而它是单位 3-球面 S^3 上的一个刚体运动．
   (b) 用类似于描述正交表示的方法证明 Q 是正交的：将对应于两个矩阵 P，$P' \in SU_2$ 的两个向量(x_1, x_2, x_3, x_4)，(x_1', x_2', x_3', x_4')的点积用矩阵作用表达出来．
   (c) 确定描述由固定矩阵 P 给出的 SU_2 上的共轭作用的矩阵．

*13. (a) 设 H_i 是 SO_3 关于 x_i-轴旋转的子群，其中 $i=1, 2, 3$．证明 SO_3 的每个元素可以写为乘积 ABA'，其中 A，$A' \in H_1$ 而 $B \in H_2$．证明只要 $B \neq I$，这个表示是唯一的．
   (b) 从几何上描述双陪集 H_1QH_1．

*14. 设 H_i 是 SO_3 关于 x_i-轴旋转的子群．证明每个元素 $Q \in SO_3$ 可以写成 $A_1A_2A_3$ 的形式，其中 $A_i \in H_i$．

第四节 特殊线性群 $SL_2(\mathbb{R})$

1. 设 $G=SL_2(\mathbb{C})$．使用 G 在$\mathbb{C}^2$ 中射线$\{rX \mid r \in \mathbb{R}, r>0\}$上的作用，证明 G 与积 $SU_2 \times H$ 同胚，其中 H 是射线$\{re_1\}$的稳定子，并具体描述 H．
2. (a) 证明法则 P，$A \rightsquigarrow PAP^*$ 定义 $SL_2(\mathbb{C})$在由所有埃尔米特矩阵组成的空间 W 上的一个作用．

301

(b) 证明函数$\langle A, A'\rangle=\det(A+A')-\det A-\det A'$是$W$上的双线性型，其符号差是(3，1).

(c) 用(a)和(b)定义一个其核为$\{\pm I\}$的同态$\varphi: SL_2(\mathbb{C})\longrightarrow O_{3,1}$.

*(d) 证明φ的象是$O_{3,1}$的单位元的连通分支.

3. 设P是$SO_3(\mathbb{C})$的矩阵.

(a) 证明1是P的一个特征值.

(b) 设X_1，X_2是P的特征向量，特征值为λ_1，λ_2. 证明只要$\lambda_1\neq\lambda_2^{-1}$，便有$X_1^t X_2=0$.

(c) 证明如果X是特征值为1的特征向量且$P\neq I$，则$X^t X\neq 0$.

4. 设$G=SO_3(\mathbb{C})$.

(a) 证明用G的左乘是在使$X^t X=1$的向量X的集合上的可迁作用.

(b) 求用G的左乘下e_1的稳定子.

(c) 证明G是路连通的.

第五节　单参数子群

1. 确定由$\mathbb{C}^+$到$SL_n(\mathbb{C})$的可微同态.
2. 描述$\mathbb{C}^\times$的所有单参数子群.
3. 用方程描述实2×2对角矩阵群的所有单参数子群的象，并作一个简洁的图示说明.
4. 设φ：$\mathbb{R}^+\longrightarrow SL_n(\mathbb{R})$是单参数子群. 证明$\ker\varphi$或者平凡，或为整个群，或者是无限循环群.
5. 求矩阵A的条件，使得e^{tA}是特殊酉群SU_n的单参数子群，并计算该群的维数.
6. 设G是形如$\begin{bmatrix} x & y \\ & 1\end{bmatrix}$($x>0$)的实矩阵的子群.

(a) 确定使e^{tA}是G的单参数子群的矩阵A.

(b) 对(a)中确定的矩阵具体计算e^A.

(c) 在(x，y)平面图示说明单参数子群.

7. 证明SU_2的单参数子群的象是T的共轭(见第三节). 用此给出这些共轭是经的一个另外的证明.
8. 确定U_2的单参数子群.
9. 设$\varphi(t)=e^{tA}$是G的单参数子群. 证明$\mathrm{im}\varphi$的陪集是微分方程$\dfrac{dX}{dt}=AX$的矩阵解.
10. $GL_n(\mathbb{R})$的单参数子群能穿过自己吗?

*11. 确定SO_2到$GL_n(\mathbb{R})$的可微同态.

第六节　李代数

1. 假设A可逆，计算$(A+B\varepsilon)^{-1}$.
2. 计算平面曲线$y^2=x^3$在点(1，1)处和在点(0，0)处的无穷小切向量.
3. (a) 画出曲线C：$x_2^2=x_1^3-x_1^2$的略图.

(b) 证明当删去原点后，这个轨迹是一个1维流形.

(c) 求C在原点处的切向量和无穷小切向量.

4. 设S是由一个方程$f=0$定义的实代数集.

(a) 证明方程$f^2=0$定义同一个轨迹S.

(b) 证明$\nabla(f^2)$在S的每个点x处为零，因而当定义方程取作$f^2=0$时，每个向量都是一个在x处的无穷小切向量.

5. 证明由$xy=1$定义的集合是对角矩阵$\begin{bmatrix} x & \\ & y\end{bmatrix}$的群的子群，并计算其李代数.

302

6. 确定酉群的李代数.
7. (a) 证明公式 $\det(I+A\varepsilon)=1+\operatorname{trace}A\varepsilon$.
   (b) 设 A 是可逆矩阵. 计算 $\det(A+B\varepsilon)$.
8. (a) 证明 O_2 通过共轭在其李代数上作用.
   (b) 证明(a)中的作用与双线性型 $\langle A, B\rangle=\frac{1}{2}\operatorname{trace}AB$ 是相容的.
   (c) 用(a)的作用定义一个同态 $O_2\longrightarrow O_2$，并具体描述这个同态.
9. 计算下面的李代数：(a) U_n；(b) SU_n；(c) $O_{3,1}$；(d) $SO_n(\mathbb{C})$. 在每一情形证明 e^{tA} 是单参数子群当且仅当 $I+A\varepsilon$ 位于群中.

*10. 利用块形式 $M=\left[\begin{array}{c|c}A&B\\\hline C&D\end{array}\right]$ 确定 $G=SP_{2n}(\mathbb{R})$ 的李代数.

11. (a) 证明如果括号定义为交叉积 $[X, Y]=X\times Y=(x_2y_3-y_2x_3,\ x_3y_1-y_1x_3,\ x_1y_2-x_2y_1)$，则 $\mathbb{R}^3$ 成为一个李代数.
    (b) 证明这个李代数同构于 SO_3 的李代数.

303

12. 对所有维数 $\leqslant 3$ 的复李代数进行分类.

*13. 线性群 G 的伴随表示 $G\times L\longrightarrow L$ 是在其李代数上通过共轭定义为 $P, A \rightsquigarrow PAP^{-1}$ 的表示. L 上的型 $\langle A, A'\rangle=\operatorname{trace}(AA')$ 称为基灵型. 对下列每个群，验证如果 $P\in G$ 且 $A\in L$，则 $PAP^{-1}\in L$，并证明基灵型是对称的和双线性的，且作用与型相容，即 $\langle A, A'\rangle=\langle PAP^{-1}, PA'P^{-1}\rangle$.
    (a) SO_n (b) SU_n (c) $O_{3,1}$ (d) $SO_n(\mathbb{C})$ (e) $SP_{2n}(\mathbb{R})$

14. 证明(a) SU_n 和(b) SO_n 的李代数上的基灵型是负定的.
15. 求 $SL_n(\mathbb{R})$ 的李代数上的基灵型的符号差.
16. (a) 利用 SU_n 的伴随表示定义同态 $\varphi: SU_n\longrightarrow SO_m$，其中 $m=n^2-1$.
    (b) 证明当 $n=2$ 时这个表示等价于第三节定义的正交表示.
17. 利用 $SL_2(\mathbb{C})$ 的伴随表示定义同构 $SL_2(\mathbb{C})/\{\pm I\}\approx SO_3(\mathbb{C})$.

第七节 群的平移

1. 计算下列群的维数.
   (a) SU_n (b) $SO_n(\mathbb{C})$ (c) $SP_{2n}(\mathbb{R})$ (d) $O_{3,1}$
2. 利用指数求方程 $P^2=I$ 在 I 附近的所有解.
3. 求 $GL_2(\mathbb{R})$ 的一个 2-维路连通的非阿贝尔子群.
4. (a) 证明每个正定埃尔米特矩阵 A 是另一个正定埃尔米特矩阵 B 的平方.
   (b) 证明 B 由 A 唯一确定.

*5. 设 A 是非奇异矩阵，并设 B 是满足 $B^2=AA^*$ 的正定埃尔米特矩阵.
   (a) 证明 A^*B^{-1} 是酉的.
   (b) 证明极分解：每个非奇异矩阵 A 是积 $A=PU$，其中 P 是正定埃尔米特的而 U 是酉的.
   (c) 证明极分解是唯一的.
   (d) 关于用酉群 U_n 在群 GL_n 上的左乘作用表明什么？

*6. 对实矩阵叙述并证明关于极分解的一个类似结论.

*7. (a) 证明指数映射定义了一个由所有埃尔米特矩阵组成的集合和由正定埃尔米特矩阵组成的集合之间的双射.
   (b) 用极分解及(a)描述 $GL_n(\mathbb{C})$ 的拓扑结构.

8. 设 B 是可逆矩阵. 刻画使 $P=e^A$ 为 B 的中心化子的矩阵 A.

*9. 设 S 表示迹为 r 的矩阵 $P\in SL_2(\mathbb{R})$ 的集合. 这些矩阵可记为 $\begin{bmatrix} x & y \\ z & r-x \end{bmatrix}$ 的形式，其中 (x, y, z) 在二次曲面 $x(r-x)-yz=1$ 上.

(a) 证明二次曲面或为单叶或双叶的抛物面，或是一个圆锥，并确定对应于每个类型的 r 的值.

304 (b) 对每一情形，确定将二次曲面分解成为共轭类的分解.

(c) 拓广定理(7.11)的证明方法以证明 $SL_2(\mathbb{R})$ 的真的正规子群只有 $\{\pm I\}$.

10. 当 $A=1+i$ 时画出群 $\mathbb{C}^\times$ 的切向量场 PA.

第八节 单群

1. 下列 $GL_n(\mathbb{C})$ 的子群中哪些是复代数群？

(a) $GL_n(\mathbb{Z})$ (b) SU_n (c) 上三角矩阵

2. (a) 写出定义 $SO_n(\mathbb{C})$ 的矩阵元素的多项式函数.

(b) 写出定义辛群的多项式方程.

(c) 证明酉群 U_n 可由其矩阵元素的实部和虚部的实多项式方程定义.

3. 确定群 $SL_n(\mathbb{R})$ 和 $SL_n(\mathbb{C})$ 的中心.

4. 描述同构(a) $PSL_2(\mathbb{F}_2)\approx S_3$ (b) $PSL_2(\mathbb{F}_3)\approx A_4$.

5. 求群 $GL_2(\mathbb{F}_3)$ 的共轭类.

6. 证明对任意特征为 2 的域 F 有 $SL_2(F)=PSL_2(F)$.

7. (a) 确定 $GL_2(\mathbb{C})$ 中包含中心 $Z=\{cI\}$ 的所有正规子群.

(b) 对 $GL_2(\mathbb{R})$ 做同样的事.

8. 对(8.12)中的七个阶，确定使 $PSL_2(F)$ 的阶为 n 的域 F 的阶.

*9. 证明存在 3420 阶的单群.

10. (a) 设 Z 是 $GL_n(\mathbb{C})$ 的中心. $PSL_n(\mathbb{C})$ 是否同构于 $GL_n(\mathbb{C})/Z$?

(b) 用 $\mathbb{R}$ 代替 $\mathbb{C}$ 回答与(a)相同的问题.

11. 证明 $PSL_2(\mathbb{F}_5)$ 同构于 A_5.

*12. 分析定理(8.3)的证明以证明除了 $F=\mathbb{F}_2$ 以外，当 F 是一个特征为 2 的域时 $PSL_2(F)$ 是一个单群.

13. (a) 设 P 是属于 SO_n 中心的矩阵，并设 A 是斜对称矩阵. 通过将矩阵函数 e^{At} 微分证明 $PA=AP$.

(b) 证明 SO_n 的中心当 n 为奇数时是平凡的，而当 n 是偶数且 $n\geq 4$ 时为 $\{\pm I\}$.

14. 计算下列群的阶.

(a) $SO_2(\mathbb{F}_3)$ 和 $SO_3(\mathbb{F}_3)$

(b) $SO_2(\mathbb{F}_5)$ 和 $SO_3(\mathbb{F}_5)$

*15. (a) 考虑 $SL_2(\mathbb{C})$ 通过共轭在复 2×2 矩阵空间 V 上的作用. 证明对于 V 的基 $(e_{11}, e_{12}, e_{21}, e_{22})$，由 $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 给出的共轭的矩阵具有块矩阵 $\begin{bmatrix} aB & bB \\ cB & dB \end{bmatrix}$ 的形式，其中 $B=(A^t)^{-1}=\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$.

(b) 证明这一作用定义一个同态 $\varphi: SL_2(\mathbb{C})\longrightarrow GL_4(\mathbb{C})$，并且 φ 的象同构于 $PSL_2(\mathbb{C})$.

(c) 通过求 4×4 矩阵的元素 y_{ij} 的多项式方程使其解正好是 $\mathrm{im}\varphi$ 中的矩阵而证明 $PSL_2(\mathbb{C})$ 是代数群.

*16. 证明 $PSL_n(\mathbb{C})$ 是单群.

305 *17. 不存在阶为 $2^5\cdot 7\cdot 11$ 的单群. 假设这一点成立，确定非阿贝尔单群的比 2448 大的最小的阶.

杂题

1. 四元数是形如 $\alpha=a+bi+cj+dk$ 的表达式，其中 $a, b, c, d\in\mathbb{R}$. 它们可以相加并用四元数群的乘法法则相乘[第二章(2.12)].

(a) 设 $\overline{\alpha}=a-bi-cj-dk$. 计算 $\alpha\overline{\alpha}$.

(b) 证明每一 $\alpha\neq0$ 有一个乘法的逆.

(c) 证明使得 $a^2+b^2+c^2+d^2=1$ 的四元数 α 的集合在乘法下构成一个与 SU_2 同构的子群.

2. 仿射群 $A_n=A_n(\mathbb{R})$ 是由 $GL_n(\mathbb{R})$ 和平移：$t_a=x+a$ 的群 T_n 生成的 $(x_1,\cdots,x_n)$ 的坐标变换的群. 证明 T_n 是 A_n 的正规子群且 A_n/T_n 同构于 $GL_n(\mathbb{R})$.

3. 凯莱变换：设 U 表示使得 $I+A$ 可逆的矩阵 A 的集合，并定义 $A'=(I-A)(I+A)^{-1}$.

(a) 证明如果 $A\in U$，则 $A'\in U$ 并证明 $A''=A$.

(b) 用 V 表示由实的斜对称 $n\times n$ 矩阵组成的向量空间. 证明法则 $A\rightsquigarrow(I-A)(I+A)^{-1}$ 定义 V 中 0 的一个邻域到 SO_n 中 I 的一个邻域的一个同胚.

(c) 找到一个对于酉群的类似断言.

(d) 设 $J=\begin{bmatrix}0 & I\\ -I & 0\end{bmatrix}$. 证明一个矩阵 $A\in U$ 是辛的当且仅当 $A'^{t}J=-JA'$.

*4. 设 $p(t)=t^2-ut+1$ 为一个二次多项式，其系数属于域 $F=\mathbb{F}_p$.

(a) 证明如果 p 在 F 中有两个不同的根，则以 p 为特征多项式的矩阵构成 $SL_2(F)$ 中的两个共轭类，并确定其阶.

(b) 证明如果 p 有两个相等的根，则以 p 为特征多项式的矩阵构成 $SL_n(F)$ 中的三个共轭类，并确定其阶.

(c) 假设 p 在 F 中没有根. 确定矩阵 $A=\begin{bmatrix} & -1\\ 1 & u\end{bmatrix}$ 在 $SL_2(F)$ 中的中心化子，并计算 A 的共轭类的阶.

(d) 求 $SL_2(\mathbb{F}_3)$ 和 $SL_2(\mathbb{F}_5)$ 的类方程.

(e) 求 $PSL_2(\mathbb{F}_3)$ 和 $PSL_2(\mathbb{F}_5)$ 的类方程，并使你的答案与 A_4 及 A_5 的类方程相一致.

(f) 计算 $SL_2(\mathbb{F}_7)$ 和 $PSL_2(\mathbb{F}_7)$ 的类方程. 用 $PSL_2(\mathbb{F}_7)$ 的类方程证明该群是单的.

306

第九章 群 表 示

在一个多世纪里数学家花费了巨大的努力来清除群论中的混乱.
然而我们仍不能回答一些最简单的问题.

Richard Brauer

第一节 群表示的定义

第五章我们学习了群在一个任意集合上的作用. 本节考虑群元素在一个向量空间上作为线性算子作用的情形. 这样的一个作用定义了 G 到一般线性群的一个同态. 到一般线性群的一个同态称为一个**矩阵表示**.

有限旋转群是应该牢记的很好的例子. 例如, 正四面体的旋转群 T 通过旋转在三维空间 V 上作用. 在第五章没有具体写出代表这个作用的矩阵; 我们现在把它写出来. 一个自然的基的选择使之具有过其三条边的中点的坐标轴, 如下图所示.

【1.1】图

设 $y_i \in T$ 表示绕一条边转过 π 的旋转, 并设 $x \in T$ 表示绕前面的顶点转过 $2\pi/3$ 的旋转. 则表示这些作用的矩阵是

【1.2】
$$R_{y_1} = \begin{bmatrix} 1 & & \\ & -1 & \\ & & -1 \end{bmatrix}, \quad R_{y_2} = \begin{bmatrix} -1 & & \\ & 1 & \\ & & -1 \end{bmatrix}, \quad R_{y_3} = \begin{bmatrix} -1 & & \\ & -1 & \\ & & 1 \end{bmatrix},$$
$$R_x = \begin{bmatrix} & & 1 \\ 1 & & \\ & 1 & \end{bmatrix}.$$

旋转 $\{y_i, x\}$ 生成群 T, 而矩阵 $\{R_{y_i}, R_x\}$ 生成一个同构的矩阵群.

具体写出代表 C_n, D_n 和 O 的作用的矩阵也是容易的, 但 I 的是相当复杂的.

群 G 的一个 n-维**矩阵表示**是一个同态

【1.3】
$$R: G \longrightarrow GL_n(F),$$

其中 F 是一个域. 我们用记号 R_g 表示元素 g 的象. 因而每个 R_g 是一个可逆矩阵, 且 G 的乘法变到矩阵乘法; 即 $R_{gh} = R_g R_h$. 矩阵(1.2)描述了 T 的一个三维矩阵表示. 它正好为忠实的, 也就是说 R 是单射, 从而将 T 同构地映到其象, 即映到 $GL_3(\mathbb{R})$ 的一个子群上. 矩阵表示并

307

不要求是忠实的.

当研究表示时，本质上尽可能不用固定的基，为此，我们引入群在一个有限维向量空间 V 上的表示的概念. 用

【1.4】 $$GL(V)$$

记 V 上可逆线性变换群，乘法法则是通常的函数合成. V 的基的选择定义了这个群与可逆矩阵群的同构：

【1.5】 $$GL(V) \longrightarrow GL_n(F)$$
$$T \rightsquigarrow T \text{ 的矩阵}.$$

G 在 V 上的一个表示指的是一个同态

【1.6】 $$\rho: G \longrightarrow GL(V).$$

表示 ρ 的维数定义为向量空间 V 的维数. 我们只讨论有限维向量空间上的表示.

矩阵表示可以视为 G 在列向量空间 F^n 上的表示.

设 ρ 是一个表示. 我们将元素 g 在 $GL(V)$ 中的象记作 ρ_g. 这样 ρ_g 是 V 上的线性算子，且 $\rho_{gh} = \rho_g \rho_h$. 如果给定基 $\boldsymbol{B} = (v_1, \cdots, v_n)$，则表示 ρ 通过法则

【1.7】 $$R_g = \rho_g \text{ 的矩阵}$$

定义一个矩阵表示. 与第四章(3.1)一样，可用符号把这个矩阵记为

【1.8】 $$\rho_g(\boldsymbol{B}) = \boldsymbol{B} R_g.$$

如果 X 是一个向量 $v \in V$ 的坐标向量，即如果 $v = \boldsymbol{B}X$，则

【1.9】 $$R_g X \text{ 是 } \rho_g(v) \text{ 的坐标向量}.$$

旋转群是实向量空间 V 上不涉及基的选择的表示的例子. 旋转是 $GL(V)$ 上的线性算子. 在(1.1)中我们选定 V 的一个基，由此 T 的元素实现为矩阵(1.2)而得到矩阵表示.

因而如果愿意选择一个基，G 在一个有限维向量空间的所有表示都可变为矩阵表示. 为了作具体计算我们会需要选择一个基，但其后必须研究当改变基的时候会发生什么，哪些性质与基的选择无关，哪个选择好一些.

V 的由矩阵 P 给出的基变换将矩阵表示 R 变为共轭表示 $R' = PRP^{-1}$，即

【1.10】 $$\text{对每个 } g \text{ 有 } R'_g = PR_gP^{-1}.$$

这由第四章基变换法则(3.4)得到.

一个等价的概念是群 G 在向量空间 V 上的作用. 当提到在一个向量空间上的作用时，我们总是指与向量空间结构相容的作用——不然就不应把 V 视为向量空间. 因而这样的一个作用是一个通常意义下的群作用[第五章(5.1)]：对所有 $g, h \in G$ 及所有 $v \in V$，有

【1.11】 $$1v = v \quad \text{且} \quad (gh)v = g(hv).$$

另外，要求每个群元素都在 V 上作为线性算子作用. 写出来就得到了法则

【1.12】 $$g(v + v') = gv + gv' \quad \text{及} \quad g(cv) = cgv,$$

这两个规则加上(1.11)，给出了 G 在向量空间 V 上的作用的全部公理. 因为群在 V 的底集上作用，我们也可像前面一样考虑其轨道和稳定子.

“G 在 V 上的作用”和“G 在 V 上的表示”这两个概念是等价的，这与 G 在集合 S 上的作用

308

等价于一个置换表示(第五章第 8 节)的理由相同：给定 G 在 V 上的表示一个 ρ，我们用法则

309 【1.13】
$$gv = \rho_g(v)$$

定义一个作用，并且反过来，给定一个作用，同样的公式可用于对所有 $g\in G$ 定义算子 ρ_g. 因为(1.12)，故它是线性算子，而且结合律(1.11)表明 $\rho_g\rho_h=\rho_{gh}$.

这样对 g 在 v 上的作用有两个记号(1.13)，我们将交替使用它们. 记号 gv 更为紧凑，我们会尽可能地使用它.

为集中我们的注意力，也是因为它容易于处理，在本章后面我们将集中讨论复表示. 因此出现的向量空间 V 应解释为复向量空间，而 GL_n 将表示复一般线性群 $GL_n(\mathbb{C})$. 每一个实矩阵表示，比如旋转群 T 的三维表示(1.2)可定义一个复表示，这只需简单地将其解释为复矩阵就行了. 我们将这样做而不作更多的解释.

第二节　G-不变型及酉表示

矩阵表示 R: $G\longrightarrow GL_n$ 称为酉的，如果所有矩阵 R_g 都是酉的，也就是同态 R 的象包含在酉群中. 换言之，一个酉表示是从 G 到酉群的同态

【2.1】
$$R:G\longrightarrow U_n.$$

本节我们证明关于有限群表示的下面这个值得注意的事实.

【2.2】定理

(a) GL_n 的每个有限子群与 U_n 的一个子群共轭.

(b) 有限群 G 的每个矩阵表示 R: $G\longrightarrow GL_n$ 共轭于一个酉表示. 换言之，给定 R，存在矩阵 $P\in GL_n$，使得对每个 $g\in G$，$PR_gP^{-1}\in U_n$.

【2.3】推论

(a) 设 A 是 GL_n 中的有限阶可逆矩阵，即对某个 r 有 $A^r=I$. 则 A 可对角化：存在 $P\in GL_n$ 使得 PAP^{-1} 是对角的.

(b) 设 $R:G\longrightarrow GL_n$ 是有限群 G 的一个表示. 则对每个 $g\in G$，R_g 是可对角化的矩阵.

推论的证明 (a) 矩阵 A 生成 GL_n 的有限子群. 由定理(2.2)，这个子群与酉群的一个子群共轭. 因此 A 与一个酉矩阵共轭. 正规算子的谱定理[第七章(7.3)]告诉我们酉矩阵可对角

310 化. 因而 A 可对角化.

(b) 推论的第二部分由第一部分得到，因为有限群的每个元素 g 的阶有限. 由于 R 是同态，R_g 也是有限阶的. ■

定理(2.2)的两部分或多或少是相同的. 我们可以把有限群到 GL_n 的包含映射视为群的矩阵表示而由(b)导出(a). 反过来，将(a)用于 R 的象可得到(b).

为了证明(b)，我们用不使用基的语言将其复述如下. 考虑一个埃尔米特空间 V(具有正定埃尔米特型 $\langle\, ,\rangle$ 的一个复空间). V 上的线性算子是酉的，如果对所有 v，$w\in V$ 有 $\langle v,w\rangle=\langle T(v),T(w)\rangle$[第七章(5.2)]. 因而很自然地把一个表示 ρ: $G\longrightarrow GL(V)$ 称为酉的，如果对所有 v，$w\in V$ 和 $g\in G$ 有

【2.4】
$$\langle v,w\rangle=\langle \rho_g(v),\rho_g(w)\rangle.$$

假设基是标准正交的，则与一个酉表示 ρ 相伴的矩阵表示 R 在(2.1)的意义下是酉的. 这可由第七章(5.2b)得到.

为了简化记号，我们将条件(2.4)写作

【2.5】
$$\langle v,w\rangle=\langle gv,gw\rangle.$$

现在将这个公式反过来，并将其视为型的条件而不是作用的条件. 给定 G 在向量空间 V 上的表示 ρ，V 上的一个型 $\langle\,,\rangle$ 称为 G-不变的，如果(2.4)成立，或者等价地，(2.5)成立.

【2.6】定理 设 ρ 是有限群 G 在复向量空间 V 上的一个表示. 在 V 上存在一个 G-不变的正定埃尔米特型 $\langle\,,\rangle$.

证明 我们从 V 上任意一个正定埃尔米特型开始；比如记这个型为 $\{\,,\}$. 我们将用这个型通过群上的平均定义一个 G-不变型. G 上的平均是一个一般方法，后面还会用得到. 在第五章(3.2)，我们已用它来求得一个有限群在平面上作用的不动点. 我们想要的型是用法则

【2.7】
$$\langle v,w\rangle=\frac{1}{N}\sum_{g\in G}\{gv,gw\}$$

定义的，其中 $N=|G|$ 是群 G 的阶. 正规化因子 $\frac{1}{N}$ 是常用的，但并不重要. 定理(2.6)可由下面这个引理得到：

【2.8】引理 型(2.7)是埃尔米特的、正定的和 G-不变的.

证明 前两个性质的验证完全是直接的. 例如，

$$\{gv,g(w+w')\}=\{gv,gw+gw'\}=\{gv,gw\}+\{gv,gw'\}.$$

311

因此

$$\begin{aligned}\langle v,w+w'\rangle&=\frac{1}{N}\sum_{g\in G}\{gv,g(w+w')\}=\frac{1}{N}\sum_{g\in G}\{gv,gw\}+\frac{1}{N}\sum_{g\in G}\{gv,gw'\}\\&=\langle v,w\rangle+\langle v,w'\rangle.\end{aligned}$$

要证型 $\langle\,,\rangle$ 是 G-不变的，设 g_0 是 G 的一个元素. 我们必须证明 $\langle g_0v,g_0w\rangle=\langle v,w\rangle$ 对所有 $v,w\in V$ 成立. 由定义，

$$\langle g_0v,g_0w\rangle=\frac{1}{N}\sum_{g\in G}\{gg_0v,gg_0w\}.$$

分析这样的和有一个非常重要的技巧，它基于用 g_0 的右乘是一个双射 $G\longrightarrow G$ 这样一个事实. 随着 g 取遍整个群，gg_0 也以不同顺序取遍整个群. 我们改变记号，用 g' 代替 gg_0. 则在和式中，g' 取遍整个群. 因此可以记和是取自 $g'\in G$ 而不是 $g\in G$. 这仅仅改变了和中各项的顺序. 于是

$$\langle g_0v,g_0w\rangle=\frac{1}{N}\sum_{g\in G}\{gg_0v,gg_0w\}=\frac{1}{N}\sum_{g\in G}\{g'v,g'w\}=\langle v,w\rangle,$$

这正是所要求的. 请考虑一下这个重新排列指标的技巧并加以理解. ■

定理(2.2)很容易就由定理(2.6)得到. 任意同态 $R: G\longrightarrow GL_n$ 是与表示相伴的矩阵表示(这时 $V=\mathbb{C}^n$ 而 $\boldsymbol{B}=\boldsymbol{E}$). 由定理(2.6)，存在 V 上一个 G-不变型 $\langle\,,\rangle$，选取 V 关于这个型的一个标准正交基. 通过这个基得到的矩阵表示 R' 与 R 共轭(1.10)并且是酉的[第七章(5.2)].

【2.9】例 矩阵 $A=\begin{bmatrix}-1 & -1\\ 1 & 0\end{bmatrix}$的阶为 3，因而它定义一个 3 阶循环群 G 的矩阵表示$\{I, A, A^2\}$. 平均化过程(2.7)由$\mathbb{C}^2$ 的标准埃尔米特积 X^*Y 产生一个 G-不变型. 它就是

【2.10】
$$\langle X,Y\rangle=\frac{1}{3}[X^*Y+(AX)^*(AY)+(A^2X)^*(A^2Y)]=X^*BX,$$
其中

【2.11】
$$B=\frac{1}{3}[I+A^*A+(A^2)^*(A^2)]=\frac{2}{3}\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}.$$

第三节 紧 群

一个线性群称为紧的，如果它是矩阵空间的闭的有界子集[附录(3.8)]. 最重要的紧群是 312 正交群和酉群：

【3.1】命题 *正交群和酉群是紧群.*

证明 正交矩阵 P 的列构成一个标准正交基，因而它们长度为 1. 因此所有矩阵元素的绝对值$\leqslant 1$. 这说明了 O_n 包含在由不等式 $|p_{ij}|\leqslant 1$ 定义的盒子里面. 因而它是有界集合. 由于它是定义为连续函数的公共零点集合，故它也是闭的，因而是紧的. 酉群的证明是相同的. ■

第二节的主要定理(2.2)和(2.6)不需做太大的改动就可以搬到紧线性群上. 作为例子我们将作出圆群 $G=SO_2$ 的情形. 在第五章中平面转过角度 θ 的旋转记作 ρ_θ. 这里将考虑 G 的一个任意的表示. 为避免混乱，我们用角度 θ 而不是 ρ_θ 表示元素

【3.2】
$$\begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}\in SO_2.$$

公式(3.2)定义群的一个特别的矩阵表示，但还有其他的矩阵表示.

假设给定一个 G 在有限维空间 V 的一个连续表示 σ，不一定是表示(3.2). 因为群律是角度的相加，σ 使用的法则是 $\sigma_{\theta+\eta}=\sigma_\theta\sigma_\eta$. 说作用是连续的是指如果选择了 V 的一个基，由此 θ 在 V 上的作用表示为某个矩阵 S_θ，则 S 的元素是 θ 的连续函数.

我们试着复制(2.6)的证明. 要在无限群上求平均，我们用积分代替求和. 选取 V 上任意一个正定的埃尔米特型$\{\ ,\ \}$，用法则

【3.3】
$$\langle v,w\rangle=\frac{1}{2\pi}\int_0^{2\pi}\{\sigma_\theta v,\sigma_\theta w\}\mathrm{d}\theta$$

定义一个新的型. 这个型具有所需要的性质. 为检验其 G-不变性，固定任意元素 $\theta_0\in G$，并设 $\eta=\theta+\theta_0$. 则 $\mathrm{d}\eta=\mathrm{d}\theta$. 因而

【3.4】
$$\langle\sigma_{\theta_0}v,\sigma_{\theta_0}w\rangle=\frac{1}{2\pi}\int_0^{2\pi}\{\sigma_\theta\sigma_{\theta_0}v,\sigma_\theta\sigma_{\theta_0}w\}\mathrm{d}\theta$$
$$=\frac{1}{2\pi}\int_0^{2\pi}\{\sigma_\eta v,\sigma_\eta w\}\mathrm{d}\eta=\langle v,w\rangle,$$

这正是要证明的.

我们不会将证明搬到一般群上，因为在一个给定的紧群 G 中找到类似于 $\mathrm{d}\theta$ 的合适的体积

元需要做一些艰巨的工作. 在(3.4)的计算中, $d\theta=d(\theta+\theta_0)$是关键的, 而幸运的是, 显然可以运用积分.

对任意紧群G存在一个称为哈尔测度的体积元dg, 它具有平移不变的性质: 如果$g_0\in G$是固定的且$g'=gg_0$, 则

313

【3.5】
$$dg=dg'.$$

利用这个测度, 可以运用上面的证明. 我们不证明哈尔测度的存在性, 但在哈尔测度存在的假设下, 用与(2.8)相同的推理可以证明(2.6)和(2.2)的如下类似的结论:

【3.6】推论 设G是GL_n的一个紧子群. 则

(a) 设σ是G在有限维向量空间V上的表示. 存在一个V上的G不变的正定埃尔米特型$\langle ,\rangle$.

(b) G的每一个连续的矩阵表示R与一个酉表示共轭.

(c) GL_n的每一个紧子群G与U_n的一个子群共轭.

第四节 G-不变子空间与既约表示

给定有限群G在向量空间V上的表示, 推论(2.3)告诉我们对每个群元素g, 存在V的一个基使得算子ρ_g的矩阵是对角的. 显然, 如果存在单独一个基, 对所有群元素g使ρ_g同时对角化将是非常方便的. 但这样的一个基并不经常存在, 因为任意两个对角矩阵是相互交换的. 为了同时对角化所有ρ_g的矩阵, 这些作用必须是交换的. 由此得到具有由对角矩阵给出的忠实表示的任意群G是阿贝尔群. 我们在后面(第八节)将看到其逆也对. 如果G是有限阿贝尔群, 则G的每一矩阵表示R都是可对角化的; 即存在单独一个矩阵P, 使得对所有$g\in G$, PR_gP^{-1}是对角的. 本节将讨论对有限群一般能做些什么.

设ρ是一个群G在向量空间V上的一个表示. V的一个子空间称为G-不变的, 如果

【4.1】
$$\text{对所有 } w\in W \text{ 和 } g\in G \text{ 有 } gw\in W.$$

于是每个群元素g的作用必将W变到自身, 即$gW\subset W$. 这是第四章第三节引入的T-不变子空间概念的一个拓广. 在一个表示中, G的元素代表V上的线性算子, 对这些算子中的每一个, 我们要求W都是一个不变子空间. 如果W是G-不变的, G在V上的作用将限制为在W上的一个作用.

作为一个例子, 考虑由一个正n-边形Δ的对称定义的二面体群[第五章(9.1)]的三维表示. 这里$G=D_n$. 有两个真的G-不变子空间: 包含Δ的平面和与Δ垂直的直线. 另一方面, 对四面体群T的表示(1.2), 不存在真的T-不变子空间, 因为没有在T的每个元素作用下都变到自身的直线或平面.

314

如果群G在一个非零向量空间V上的一个表示ρ没有真的G-不变子空间, 则称它为一个既约表示. 如果存在一个真的不变子空间, 则ρ称为可约的. T的标准三维表示是既约的.

当V是G-不变子空间的直和时: $V=W_1\oplus W_2$, V上的表示ρ称为是它在W_i上的限制ρ_i的直和, 并记作

【4.2】
$$\rho=\rho_1\oplus\rho_2.$$

假设是这一情形. 选择W_1, W_2的基$\mathbf{B}_1$, $\mathbf{B}_2$, 并设$\mathbf{B}=(\mathbf{B}_1, \mathbf{B}_2)$是通过将这两个基按顺序排

列得到的 V 的基[第三章(6.6)]. 则 ρ_g 的矩阵 R_g 具有块形式

【4.3】
$$R_g=\left[\begin{array}{c|c} A_g & 0 \\ \hline 0 & B_g \end{array}\right],$$

其中 A_g 是 ρ_{1g} 关于基 $\boldsymbol{B}_1$ 的矩阵而 B_g 是 ρ_{2g} 关于基 $\boldsymbol{B}_2$ 的矩阵. 反之，如果矩阵 R_g 有这样的块形式，则表示是一个直和.

例如，考虑旋转群 $G=D_n$ 通过正 n-边形 Δ 的对称在 $\mathbb{R}^3$ 上的作用. 如果选择一个标准正交基 $\boldsymbol{B}$ 使得 v_1 与 Δ 的平面垂直且 v_2 过一个顶点，则对应于标准生成元 x，y[第五章(3.6)]的旋转由矩阵

【4.4】
$$R_x=\begin{bmatrix}1 & & \\ & c_n & -s_n \\ & s_n & c_n\end{bmatrix},\quad R_y=\begin{bmatrix}-1 & & \\ & 1 & \\ & & -1\end{bmatrix}$$

表示，其中 $c_n=\cos(2\pi/n)$ 而 $s_n=\sin(2\pi/n)$. 这样 R 是一个一维表示 A

【4.5】
$$A_x=[1],\quad A_y=[-1]$$

和一个二维表示 B

【4.6】
$$B_x=\begin{bmatrix}c_n & -s_n \\ s_n & c_n\end{bmatrix},\quad B_y=\begin{bmatrix}1 & \\ & -1\end{bmatrix}$$

的直和. 表示 B 是 D_n 作为 Δ 在平面中的对称的基本二维表示.

另一方面，即使表示 ρ 是可约的，除非 V 中给定的基与直和分解相容，否则矩阵 R_g 不会有块形式. 当一个表示没有用合适的基表出时，如果不作进一步分析，将很难说一个表示是否是可约的.

【4.7】命题　*设 ρ 是 G 在一个埃尔米特向量空间 V 上的酉表示，并设 W 是一个 G-不变子空间. 正交补 $W^{\perp}$ 也是 G-不变的，并且 ρ 是它在 W 和 $W^{\perp}$ 上限制的直和.*

315

证明　设 $v\in W^{\perp}$，从而 $v\perp W$. 由于作用 ρ_g 是酉的，它们保持正交性[第七章(5.2)]，于是 $gv\perp gW$. 因为 W 是 G-不变的，$W=gW$，因而 $gv\perp W$. 于是 $gv\in W^{\perp}$. 这说明 $W^{\perp}$ 也是 G-不变的. 由第七章(2.7)，我们知道 $V=W\oplus W^{\perp}$. ■

当存在真不变子空间时这个命题使得可以将表示分解为直和. 用归纳法，我们得到下面的推论：

【4.8】推论　*埃尔米特向量空间 V 上的每一个酉表示 ρ: $G\longrightarrow GL(V)$ 是既约表示的直和.*

把这个推论与(2.2)结合起来，我们得到下面的推论：

【4.9】推论　*马什克定理：有限群 G 的每一个表示是既约表示的直和.*

第五节　特　征　标

群 G 的两个表示 ρ: $G\longrightarrow GL(V)$ 和 ρ': $G\longrightarrow GL(V')$ 称为同构的或等价的，如果存在一个与群 G 的作用相容的向量空间的同构 T: $V\longrightarrow V'$，对所有 $g\in G$ 和 $v\in V$ 有：

【5.1】
$$gT(v)=T(gv)\quad 或\quad \rho'_gT(v)=T(\rho_g(v)).$$

如果 $\boldsymbol{B}$ 是 V 的一个基而 $\boldsymbol{B}'=T(\boldsymbol{B})$ 是 V' 对应的基，则相伴的矩阵表示 R_g 与 $R_g{}'$ 是相等的.

在下面四节将关注有限群的表示．我们将会看到一个有限群有相对来说并不多的既约表示的同构类．然而，每一表示有一个复杂的矩阵描述．理解表示的秘密是除非在绝对需要的情形，否则不必具体地写出其矩阵．因此为了便于分类我们将丢掉表示 ρ 中所含有的大部分信息，而只保持最为本质的那些信息．我们所要用到的是 ρ 的迹，称为它的特征标．特征标通常记作 χ．

表示 ρ 的特征标 χ 是由

【5.2】
$$\chi(g) = \mathrm{trace}(\rho_g)$$

定义的映射 χ：$G \longrightarrow \mathbb{C}$．如果 R 是由 ρ 通过 V 的基的一个选择得到的矩阵表示，则

【5.3】
$$\chi(g) = \mathrm{trace}(R_g) = \lambda_1 + \cdots + \lambda_n,$$

其中 λ_i 是 R_g 或 ρ_g 的特征值．

特征标 χ 的维数定义为表示 ρ 的维数．既约表示的特征标称为既约特征标． 316

下面是特征标的一些基本性质．

【5.4】命题 设 χ 是有限群 G 在向量空间 V 上的表示 ρ 的特征标．

(a) $\chi(1)$是特征标的维数[V 的维数]．

(b) 对所有 g，$h \in G$，$\chi(g) = \chi(hgh^{-1})$．换言之，特征标在每一个共轭类上为常数．

(c) $\chi(g^{-1}) = \overline{\chi(g)}$[$\chi(g)$的复共轭]．

(d) 如果 χ' 是另一个表示 ρ' 的特征标，则直和 $\rho \oplus \rho'$ 的特征标是 $\chi + \chi'$．

证明 断言(a)中的符号 1 表示 G 的单位元素．这个性质是平凡的：$\chi(1) = \mathrm{trace} I = \dim V$．性质(b)成立，这是因为与 ρ 相伴的矩阵表示 R 是个同态，它表明 $R_{hgh^{-1}} = R_h R_g R_h^{-1}$，以及由于 $\mathrm{trace}(R_h R_g R_h^{-1}) = \mathrm{trace} R_g$[第四章(4.18)]．性质(d)亦是显然的，因为分块矩阵(4.3)的迹是 A_g 和 B_g 的迹的和．

性质(c)不是那么显然．如果 R_g 的特征值为 λ_1，…，λ_n，则 $R_g^{-1} = (R_g)^{-1}$ 的特征值是 λ_1^{-1}，…，λ_n^{-1}．(c)的断言为

$$\chi(g^{-1}) = \lambda_1^{-1} + \cdots + \lambda_n^{-1} = \overline{\lambda_1} + \cdots + \overline{\lambda_n} = \overline{\chi(g)},$$

要证这一点，我们利用 G 是有限群这个事实．G 的每个元素都是有限阶的．如果 $g^r = 1$，则 R_g 是一个 r 阶矩阵，于是其特征值 λ_1，…，λ_n 为单位根．这蕴涵 $|\lambda_i| = 1$，因而对每个 i 有 $\lambda_i^{-1} = \overline{\lambda_i}$． ■

为避免将循环群与共轭类混淆，我们将在本章用正体字母 C 而不是斜体字母 C 表示共轭类．这样一个元素 $g \in G$ 的共轭类记作 C_g．

为了简化特征标的计算，需要注意下面两点．首先，因为 χ 的取值仅依赖于一个元素 $g \in G$ 的共轭类，我们只需确定 χ 在每一类的一个代表元素上取值．其次，由于特征标 $\chi(g)$ 的值是算子 ρ_g 的迹且由于迹不依赖于基的选择，我们可自由地选择方便的基．而且，可以对每个单独的元素选择一个方便的基．不必对所有元素用同一个基．

作为例子，我们来确定(1.2)定义的正四面体群 T 的旋转表示的特征标 χ．T 中有四个共

轭类，它们由元素 1，x，x^2，y 代表，其中如前，x 为绕一个顶点转过 $2\pi/3$ 的旋转而 y 为绕一个边中点转过 π 的旋转．这些代表上的特征标的值可由矩阵(1.2)得出：

【5.5】 $$\chi(1)=3,\quad \chi(x)=0,\quad \chi(x^2)=0,\quad \chi(y)=-1.$$

317 把特征标看作向量有时是很有用的．可以通过把 G 的元素按某个顺序排列而做到这一点：$G=(g_1,\cdots,g_N)$；则向量表示 χ 是

【5.6】 $$\chi=(\chi(g_1),\cdots,\chi(g_N))^t.$$

因为 χ 在共轭类上是常数，自然可以通过先排列共轭类然后按某个顺序列出每个共轭类来排列 G．如果对特征标(5.5)这样做，以 C_1，C_x，C_{x^2}，C_y 这个顺序排列，得到的向量是

【5.7】 $$\chi=(3;0,0,0,0;0,0,0,0;-1,-1,-1)^t.$$

我们将不再具体写出这样的向量．

关于特征标的主要定理将它们与$\mathbb{C}^N$ 的埃尔米特点积联系起来．这是代数中最美的定理之一，既是因为其叙述本身是那样优美，也因为它将表示分类的问题大大地进行了简化．我们定义

【5.8】 $$\langle\chi,\chi'\rangle=\frac{1}{N}\sum_g\overline{\chi(g)}\chi'(g),$$

其中 $N=|G|$．设 χ，χ' 由(5.7)中的向量表示，这是用因子$\frac{1}{N}$作了正规化的标准埃尔米特积．

【5.9】定理 设 G 是 N 阶群，设 ρ_1，ρ_2，…表示 G 的互不相同的既约表示的同构类，并且设 χ_i 是 ρ_i 的特征标．

(a) 正交关系：特征标 χ_i 是标准正交的．也就是说，如果 $i\neq j$ 则$\langle\chi_i,\chi_j\rangle=0$，且对每一 i 有$\langle\chi_i,\chi_i\rangle=1$．

(b) 存在有限多个既约表示的同构类，其个数与群的共轭类的个数一样多．

(c) 设 d_i 是既约表示 ρ_i 的维数，并设 r 是既约表示的个数．则 d_i 整除 N 且

【5.10】 $$N=d_1^2+\cdots+d_r^2.$$

第九节中将证明定理中除了 d_i 整除 N 外的其他断言，而这个断言我们将不予证明．

在每个共轭类上都是常数的复值函数 $\varphi:G\longrightarrow\mathbb{C}$ 称为一个类函数．因为类函数在每个类上是常数，它也可以描述为共轭类的集合的函数．类函数构成一个复向量空间，将其记作$\mathscr{C}$．我们用(5.8)定义的型使$\mathscr{C}$构成一个埃尔米特空间．

318 **【5.11】推论** 既约特征标构成$\mathscr{C}$的标准正交基．

这由(5.9a 和 b)得到．因为特征标是正交的，故它们是线性无关的，并且因为$\mathscr{C}$的维数是共轭类的个数，也就是 r，所以它们张成空间．

这个推论使得可以利用正交投影公式[第七章(3.8)]将给定特征标分解为既约特征标的线性组合．设 χ 为表示 ρ 的特征标．由推论(4.9)，ρ 同构于既约表示 ρ_1，…，ρ_r 的直和；用符号将其记为 $\rho=n_1\rho_1\oplus\cdots\oplus n_r\rho_r$，其中 n_i 是非负整数而 $n\rho$ 代表 n 个表示 ρ 的拷贝的直和．则 $\chi=n_1\chi_1+\cdots+n_r\chi_r$．因为$(\chi_1,\cdots,\chi_r)$是标准正交基，我们有下面的结果：

【5.12】推论 设 $\chi_1, \cdots, \chi_r$ 是有限群 G 的既约特征标，并设 χ 为任意特征标. 则 $\chi = n_1\chi_1 + \cdots + n_r\chi_r$，其中 $n_i = \langle \chi, \chi_i \rangle$.

【5.13】推论 如果两个表示 ρ，ρ' 有相同的特征标，则它们是同构的.

设 χ，χ' 是两个表示 ρ，ρ' 的特征标，其中 $\rho = n_1\rho_1 \oplus \cdots \oplus n_r\rho_r$ 而 $\rho' = n_1'\rho_1 \oplus \cdots \oplus n_r'\rho_r$. 则这两个表示的特征标是 $\chi = n_1\chi_1 + \cdots + n_r\chi_r$ 和 $\chi' = n'_1\chi_1 + \cdots + n_r'\chi_r$. 由于 $\chi_1, \cdots, \chi_r$ 是线性无关的，由 $\chi = \chi'$ 可得，对每个 i 有 $n_i = n_i'$.

【5.14】推论 一个特征标 χ 具有性质 $\langle \chi, \chi \rangle = 1$ 当且仅当它是既约的.

因为如果 $\chi = n_1\chi_1 + \cdots + n_r\chi_r$，则 $\langle \chi, \chi \rangle = n_1^2 + \cdots + n_r^2$. 这个值为 1 当且仅当单独一个 n_i 是 1 而其余是零.

求 $\langle \chi, \chi \rangle$ 的值是检验表示的既约性的一个实用方法. 例如，设 χ 是表示(1.2)的特征标(5.7). 则 $\langle \chi, \chi \rangle = (3^2+1+1+1)/12 = 1$. 故 χ 既约.

定理(5.9)的(c)应与类方程[第六章(1.7)]相对照. 设 $C_1, \cdots, C_r$ 是 G 的共轭类，设 $c_i = |C_i|$ 是共轭类的阶. 则 c_i 整除 N，且 $N = c_1 + \cdots + c_r$. 虽然共轭类与既约表示有相同的个数，但它们之间准确的关系是非常难于捉摸的.

作为第一个例子，我们将确定二面体群 D_3[第五章(3.6)]的既约表示. 它有三个共轭类，$C_1 = \{1\}$，$C_2 = \{y, xy, x^2y\}$，$C_3 = \{x, x^2\}$[第六章(1.8)]，因而有三个既约表示. 方程(5.10)仅有的解是 $6 = 1^2 + 1^2 + 2^2$，因而 D_3 有两个一维表示 ρ_1，ρ_2 及一个既约二维表示 ρ_3. 每个群 G 都有平凡的一维表示(对所有 g 有 $R_g = 1$)；记之为 ρ_1. 另一个一维表示是同构于 D_3 的对称群 S_3 的符号表示：$R_g = \mathrm{sign}(g) = \pm 1$. 这是表示(4.5)；记之为 ρ_2. 二维表示由(4.6)定义，记之为 ρ_3. 319

我们通常将特征标 χ_i 列成特征标表，而不是将它们作为向量列出. 在这个表中，三个共轭类用元素 1，y，x 代表. 共轭类的阶写在它们上面. 这样 $|C_y| = 3$.

【5.15】 D_3 的特征标表

	共轭类			
	(1)	(2)	(3)	类的阶
既约特征标	1	x	y	代表元素
χ_1	1	1	1	
χ_2	1	-1	1	特征标的值
χ_3	2	0	-1	

在这样一个表中，顶行对应于平凡特征标，完全由 1 组成. 第一列包含表示的维数，这是因为 $\chi_i(1) = \dim\rho_i$.

为求双线性型(5.8)在特征标上的取值，记住在 y 的类中有三个元素而在 x 的类中有两个元素. 这样

$$\langle\chi_3,\chi_3\rangle=\frac{1}{N}\sum_g\overline{\chi_3(g)}\chi_3(g)=(1\cdot(\overline{\chi_3(1)}\chi_3(1))+3\cdot(\overline{\chi_3(y)}\chi_3(y))+2\cdot(\overline{\chi_3(x)}\chi_3(x)))/6$$
$$=(1\cdot\overline{2}\cdot 2+3\cdot\overline{0}\cdot 0+2\cdot(\overline{-1})\cdot(-1))/6=1.$$

这证实了 ρ_3 是既约的.

作为另一个例子，考虑 3 阶循环群 $C_3=\{1,x,x^2\}$. 由于 C_3 是阿贝尔的，存在三个共轭类，每个由一个元素组成. 定理(5.9)表明存在三个既约表示，每一个的维数都是 1. 设 $\zeta=\frac{1}{2}(-1+\sqrt{3}i)$是 1 的一个三次根. 三个表示为

【5.16】 $$\rho_{1_x}=1,\quad \rho_{2_x}=\zeta,\quad \rho_{3_x}=\zeta^2.$$

【5.17】 C_3 的特征标表

	1	x	x^2
χ_1	1	1	1
χ_2	1	ζ	ζ^2
χ_3	1	ζ^2	ζ

320 注意 $\overline{\zeta}=\zeta^2$. 于是

$$\langle\chi_2,\chi_3\rangle=(\overline{1}\cdot 1+\overline{\zeta}\zeta^2+\overline{\zeta^2}\zeta)/3=(1+\zeta+\zeta^2)/3=0,$$

这与正交关系是一致的.

作为第三个例子，我们确定正四面体群 T 的特征标表. 上面确定了共轭类 C_1，C_x，C_{x^2}，C_y，而且类方程是 $12=1+4+4+3$. (5.10)仅有的解是 $12=1^2+1^2+1^2+3^2$，因而存在维数为 1，1，1，3 的四个表示. T 碰巧有一个与克莱因四元群同构的 4 阶正规子群 H，而且使得商群 $\overline{T}=T/H$ 是 3 阶循环群. $\overline{T}$ 的任意表示$\overline{\rho}$ 通过合成

$$T\xrightarrow{\pi}\overline{T}\xrightarrow{\overline{\rho}}GL(V)$$

给出 T 的一个表示. 这样循环群的三个一维表示确定了 T 的表示. 它们的特征标 χ_1，χ_2，χ_3 可由(5.17)确定. 特征标(5.5)在下表中记作 χ_4.

【5.18】 T 的特征标表

	(1) 1	(4) x	(4) x^2	(3) y
χ_1	1	1	1	1
χ_2	1	ζ	ζ^2	1
χ_3	1	ζ^2	ζ	1
χ_4	3	0	0	-1

群的各种性质可以很容易地由特征标表读出. 我们忘记这是 T 的特征标表，并假设它是作为一个未知群 G 的特征标表给出的. 毕竟可以想象另一个群的同构类也会有相同的特征标.

群 G 的阶为 12，这是共轭类的阶的和. 其次，由于 ρ_2 的维数为 1，$\chi_2(y)$是 1×1 矩阵 ρ_{2_y} 的迹. 于是 $\chi_2(y)=1$ 这一事实表明也有 $\rho_{2_y}=1$，即 y 属于 ρ_2 的核. 事实上，ρ_2 的核等于两个共轭类的并 $C_1\cup C_y$. 这是 G 中的一个 4 阶子群 H. 此外，H 是克莱因四元群. 因为如果 H 是

C_4，则其唯一的 2 阶元自身就构成一个共轭类．也可由 $\chi_2(x)$ 的值得到 x 的阶被 3 整除．回到 12 阶群的列表[第六章(5.1)]，我们看到 $G \approx T$.

第六节 置换表示与正则表示

设 S 是一个集合．由通过形式线性组合

$$v = \sum_i a_i s_i, \quad a_i \in \mathbb{C}$$

的向量空间 $V=V(S)$[第三章(3.21)]，我们可从 G 在 S 上的作用构造群 G 的一个表示．元素 $g \in G$ 通过置换 S 的元素并令系数不变而作用在向量上：

321

【6.1】
$$gv = \sum_i a_i g s_i.$$

如果选择 S 的一个序 $s_1, \cdots, s_n$ 并取 V 的基 $(s_1, \cdots, s_n)$，那么 R_g 是描述 g 在 S 上作用的置换矩阵．

例如，设 $G=T$ 并设 S 是正四面体群的面的集合：$S=(f_1, \cdots, f_4)$．G 在 S 上的作用定义 G 的一个 4-维表示．设 x 表示绕一个面 f_1 转过 $2\pi/3$ 的旋转而 y 是如前面一样绕一条边转过 π 的旋转．那么如果把面适当地标号，则有

【6.2】
$$R_x = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad 和 \quad R_y = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

我们说 ρ(或 R)是与 G 在 S 上的作用相伴的表示并常常把 ρ 叫做置换表示，虽然这个说法在别处有另外的特定的含义(第五章第八节)．

如果将 G 所作用的一个集合分解成轨道，我们将得到相伴的表示作为直和的一个分解．这是显然的．但它具有一个重要的新特征：$V(S)$ 中有线性组合这一事实使我们可进一步将表示分解．即使 S 可能只有单独一条轨道，除了 S 只有一个元素的情形外，相伴的置换表示决不是既约的．这是因为向量 $w=s_1+\cdots+s_n$ 在基的每个置换之下都不变，因而 1-维向量子空间 $W=\{cw\}$ 是 G-不变的．平凡表示是每个置换表示的直和项．

容易计算置换表示的特征标：

【6.3】
$$\chi(g) = S 中由 g 保持不变的元素个数,$$

因为对每一个由置换保持不变的指标，在相伴的置换矩阵的对角线上有一个 1 而其余对角元素皆为 0．例如，T 在正四面体的面上的表示的特征标是

【6.4】

	1	x	x^2	y
χ	4	1	1	0

，

并且特征标表(5.18)表明 $\chi=\chi_1+\chi_4$．因而由推论(5.13)，$\rho \approx \rho_1 \oplus \rho_4$．作为另一个例子，$T$ 在正四面体的六条边上的作用的特征标为

【6.5】

	1	x	x^2	y
χ	6	0	0	2

再次用(5.18)，我们得到 $\chi=\chi_1+\chi_2+\chi_3+\chi_4$.

[322] G 的正则表示 ρ^{reg} 是 G 由左乘对其自身作用时得到的相伴的表示．换言之，设 $S=G$，以左乘作用．这并不是一个特别有意思的作用，但其相伴的表示是非常有意思的．其特征标 χ^{reg} 特别简单：

【6.6】 $$\chi^{reg}(1)=N,\quad 且如果\quad g\neq 1,\quad 则\ \chi^{reg}(g)=0,$$

其中 $N=G$. 第一个公式是显然成立的：$\chi(1)=\dim\rho$，而且对任意表示 ρ，$\rho^{reg}(1)$ 的维数为 N. 第二个公式由(6.3)得到，因为除了 $g=1$ 的情形以外，用 g 左乘不能保持 G 的任一元素不变.

由于这个公式，容易用正交投影公式(5.12)对任意表示 ρ 的特征标 χ 计算 $\langle\chi^{reg},\chi\rangle$. 由于 $\chi(1)=\dim\rho$，其答案是

【6.7】 $$\langle\chi^{reg},\chi\rangle=\dim\rho,$$

这使我们能将 χ^{reg} 写成既约特征标的线性组合：

【6.8】推论 $\chi^{reg}=d_1\chi_1+\cdots+d_r\chi_r$，并且 $\rho^{reg}\approx d_1\rho_1+\cdots+d_r\rho_r$，其中 d_i 是 ρ_i 的维数而 $d_i\rho_i$ 表示 d_i 个 ρ_i 的直和.

这难道不是个漂亮的公式吗？我们可以通过比较维数从(6.8)推出公式(5.10). 这表明定理(5.9)的公式(5.10)由正交关系得到.

例如，对于群 D_3，正则表示的特征标是

	1	x	y
χ^{reg}	6	0	0

表(5.15)表明 $\chi^{reg}=\chi_1+\chi_2+2\chi_3$，这正是我们所预期的.

作为另一个例子，考虑 3 阶循环群$\{1, x, x^2\}$的正则表示 R. 代表 x 的置换矩阵是

$$R_x=\begin{bmatrix} & & 1\\ 1 & & \\ & 1 & \end{bmatrix}.$$

其特征值为 1，ζ，ζ^2，其中 $\zeta=\frac{1}{2}(-1+\sqrt{3}i)$. 这样 R_x 与

$$R'_x=\begin{bmatrix} 1 & & \\ & \zeta & \\ & & \zeta^2\end{bmatrix}$$

共轭. 这个矩阵展示了正则表示分解为既约一维表示的分解 $\rho^{reg}\approx\rho_1+\rho_2+\rho_3$.

第七节 二十面体群的表示

本节我们确定二十面体群的既约特征标. 迄今为止，我们只看到其平凡表示 ρ_1 及作为旋

[323] 转群的三维表示. 用 ρ_2 表示旋转表示. I 中有五个共轭类[第六章(2.2)]，即

【7.1】
$$C_1 = \{1\},$$
$C_2 = 15$ 个转过角度 π 的旋转"x",

$C_3 = 20$ 个转过角度 $2\pi/3, 4\pi/3$ 的旋转"y",

$C_4 = 12$ 个转过角度 $2\pi/5, 8\pi/5$ 的旋转"z",

$C_5 = 12$ 个转过角度 $4\pi/5, 6\pi/5$ 的旋转"z^2",

因此存在另外三个既约表示．(5.10)仅有的解是 $d_i=1, 3, 3, 4, 5$：
$$60 = 1^2 + 3^2 + 3^2 + 4^2 + 5^2,$$
这是我们已经知道的．

将其余表示记为 ρ_3，ρ_4，ρ_5，其中 $\dim\rho_3=3$，等等．寻找缺失的既约表示的一个好办法是分解一些已知的置换表示．我们知道 I 在一个五元集上作用[第六章(2.6)]．这给出了一个五维表示 ρ'．如在第六节所见到的，平凡表示是 ρ' 的一个直和项．其正交补正好是所求的四维既约表示：$\rho'=\rho_1\oplus\rho_4$．而且 I 置换过正十二面体对面中心的六条轴．设对应的六维表示是 ρ''．则 $\rho''=\rho_1\oplus\rho_5$．我们可以通过计算 ρ_4 和 ρ_5 的特征标并应用定理(5.9)来验证这个事实．特征标 χ_4，χ_5 由每个值从 χ'，χ'' 减去 $\chi_1=1$ 得到．例如，ρ' 将 x 实现为 $\{\mathbf{1}, \cdots, \mathbf{5}\}$ 的一个 2 阶偶置换，因而它是两个不相交的对换的积，它保持一个指标不变．因而 $\chi'(x)=1$ 且 $\chi_4(x)=0$．

第二个三维表示 ρ_3 是相当费解的，因为它与 ρ_2 相当地相似．它可以这样得到：由于 I 同构于 A_5，可将其视为对称群 S_5 的正规子群．由一个不在 A_5 中的 S_5 的元素 p 给出的共轭定义了 A_5 的一个自同构 σ．这个自同构互换两个共轭类 C_4，C_5．因为其他共轭类有不同的阶，所以它们并不互换．例如，用循环记号，设 $z=(\mathbf{12345})$ 并设 $p=(\mathbf{2354})$．则 $p^{-1}zp=(\mathbf{4532})(\mathbf{12354})(\mathbf{2354})=(\mathbf{13524})=z^2$．表示 ρ_3 等于 $\rho_2\circ\sigma$．

ρ_3 的特征标由 ρ_2 的特征标通过互换 z，z^2 的值计算．算出这些特征标后，验证关系 $\langle\chi_i, \chi_j\rangle=0$ 和 $\langle\chi_i, \chi_i\rangle=1$ 表明这些表示是既约的且我们的列表是正确的．

【7.2】$I=A_5$ 的特征标表

	(1)	(15)	(20)	(12)	(12)
	1	x	y	z	z^2
χ_1	1	1	1	1	1
χ_2	3	-1	0	α	β
χ_3	3	-1	0	β	α
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

在这个表中，α 是转过角度 $2\pi/5$ 的三维旋转的迹，为
$$\alpha = 1 + 2\cos 2\pi/5 = \frac{1}{2}(-1+\sqrt{5}),$$
β 可以类似地算出：$\beta=1+2\cos 4\pi/5=\frac{1}{2}(-1-\sqrt{5})$.

324

第八节 一维表示

设 ρ 是群 G 的一个一维表示. 则 R_g 是一个 1×1 矩阵，如果将一个 1×1 矩阵与其元素等同起来，则有 $\chi(g)=R_g$. 于是在这种情形，特征标 χ 是一个同态 χ: $G\longrightarrow\mathbb{C}^\times$，即如果 $\dim\rho=1$，它满足法则

【8.1】 $$\chi(gh)=\chi(g)\chi(h).$$

这样一个特征标称为阿贝尔的. 请注意对于维数>1的特征标来说，公式(8.1)是不对的.

如果 G 是有限群，则一个阿贝尔特征标 χ 所取的值总是 1 的根：即存在 r，使得

【8.2】 $$\chi(g)^r=1,$$

这是因为元素 g 的阶有限.

一维特征标在函数乘积

【8.3】 $$\chi\chi'(g)=\chi(g)\chi'(g)$$

下构成一个群. 这个群称为 G 的特征标群并常记为$\hat{G}$. 当 G 是阿贝尔群时特征标群特别重要，因为有下面的事实：

【8.4】定理 如果 G 是有限阿贝尔群，则 G 的每个既约表示是一维的.

证明 由于 G 是阿贝尔群，每个共轭类由一个元素组成. 因而共轭类的个数为 N. 由定理(5.9)，存在 N 个既约表示，且 $d_1=d_2=\cdots=d_n=1$. ■

第九节 舒尔引理和正交关系的证明

设 ρ，ρ'是群 G 在两个向量空间 V，V'上的表示. 我们称一个线性变换 T: $V\longrightarrow V'$为 G-不变的，如果它与 G 在 V 和 V'上的两个作用相容，即如果对所有 $g\in G$ 和 $v\in V$ 有

【9.1】 $$gT(v)=T(gv),\quad 或\quad \rho'_g(T(v))=T(\rho_g(v)).$$

325 这样表示的一个同构(第五节)是一个双射的 G-不变的变换. 也可将(9.1)记为

【9.2】 $$对所有\quad g\in G\quad 有\quad \rho'_g\circ T=T\circ\rho_g.$$

设给定 V 和 V'的基 $\boldsymbol{B}$，$\boldsymbol{B}'$，并设 R_g，R'_g 及 A 为 ρ_g，ρ'_g 和 T 关于这两个基的矩阵. 则(9.2)成为

【9.3】 $$对所有\quad g\in G\quad 有\quad R'_gA=AR_g.$$

$\rho=\rho'$这一特殊情形是非常重要的. V 上的一个 G-不变线性算子 T 是一个对每个 $g\in G$ 都与 ρ_g 交换的线性算子：

【9.4】 $$\rho_g\circ T=T\circ\rho_g,\quad 或\quad R_gA=AR_g.$$

这些公式不过是当 $\rho=\rho'$时(9.2)和(9.3)的重复.

【9.5】命题 G-不变线性变换 T: $V\longrightarrow V'$的核与象分别是 V 和 V'的 G-不变子空间.

证明 任意线性变换的核与象是子空间. 我们证明 $\ker T$ 是 G-不变的：需要证明如果 $v\in\ker T$ 则 $gv\in\ker T$,或者如果 $T(v)=0$，则 $T(gv)=0$. 其实，

$$T(gv)=gT(v)=g0=0.$$

类似地，如果 $v'\in \mathrm{im}T$，则 $v'=T(v)$对某个 $v\in V$ 成立. 于是

$$gv' = gT(v) = T(gv),$$

因此亦有 $gv' \in \mathrm{im}T$. ■

【9.6】定理 舒尔引理：设 ρ，ρ' 是 G 在向量空间 V，V' 上的两个既约表示，并设 $T: V \longrightarrow V'$ 是一个 G-不变的变换.

(a) 或者 T 是同构，或者 $T=0$.

(b) 如果 $V=V'$ 且 $\rho=\rho'$，则 T 是用一个标量作的乘法.

证明 (a) 由于 ρ 是既约的且由于 $\ker T$ 是 G-不变子空间，$\ker T=V$ 或 $\ker T=0$. 在第一种情形，$T=0$. 在第二种情形，T 是单射且将 V 同构地映到其象. 于是 $\mathrm{im}T$ 是非零的. 由于 ρ' 是既约的且 $\mathrm{im}T$ 是 G-不变的，$\mathrm{im}T=V'$. 从而 T 是一个同构.

(b) 假设 $V=V'$，则 T 是 V 上的一个线性算子. 选择 T 的一个特征值 λ. 则 $(T-\lambda I)=T_1$ 亦是 G-不变的. 其核非零，因为它包含一个特征向量. 由于 ρ 是既约的，$\ker T_1=V$，这表明 $T_1=0$. 因而 $T=\lambda I$. ■

用平均化过程可以从任意线性变换 $T: V \longrightarrow V'$ 创建一个 G-不变的变换. 为此，我们将条件(9.1)重新写为 $T(v)=\rho_g'^{-1}(T(\rho_g(v)))$ 的形式，或

326

【9.7】
$$T(v) = g^{-1}(T(gv)).$$

平均是由

【9.8】
$$\tilde{T}(v) = \frac{1}{N}\sum_g g^{-1}(T(gv))$$

定义的线性算子 $\tilde{T}$，其中和前面一样，$N=|G|$. 如果给定 V，V' 的基，而且如果 ρ_g，ρ_g'，T，$\tilde{T}$ 的矩阵分别是 R_g，R_g'，A，$\tilde{A}$，则

【9.9】
$$\tilde{A} = \frac{1}{N}\sum_g R_g'^{-1} A R_g.$$

由于线性变换的合成和线性变换的和仍是线性变换，因此 $\tilde{T}$ 是线性变换. 为证它是 G-不变的，我们固定一个元素 $h\in G$ 且令 $g'=gh$. 如引理(2.8)的证明中一样改变下标，

$$\begin{aligned} h^{-1}\tilde{T}(hv) &= \frac{1}{N}\sum_g h^{-1}g^{-1}(T(ghv)) \\ &= \frac{1}{N}\sum_g g'^{-1}(T(g'v)) = \tilde{T}(v). \end{aligned}$$

因此 $\tilde{T}(hv)=h\tilde{T}(v)$. 由于 h 是任意的，这表明 $\tilde{T}(v)$ 是 G-不变的.

我们最终会碰巧得到平凡的线性变换，即虽然 T 不为零但 $\tilde{T}=0$. 事实上，舒尔引理告诉我们如果 ρ 与 ρ' 是既约的但不同构，则必然得到 $\tilde{T}=0$. 在正交关系的证明中我们将很好地利用这个看似负面的事实.

当 $\rho=\rho'$ 时，利用下面命题可证明平均常是非零的.

【9.10】命题 设 ρ 是有限群 G 在向量空间 V 上的表示，并设 $T: V \longrightarrow V'$ 是一个线性算子. 用公式(9.8)定义 $\tilde{T}$. 则 $\mathrm{trace}\,\tilde{T}=\mathrm{trace}T$. 这样如果 T 的迹非零，则 $\tilde{T}$ 亦非零.

证明 取 $R=R'$，如公式(9.9)中一样进行计算. 由于 $\mathrm{trace}A=\mathrm{trace}R_g^{-1}AR_g$，命题成立. ■

下面是一个计算范例．设 $G=C_3=\{1, x, x^2\}$，并设 $\rho=\rho'$为 G 的正则表示(第六节)，于是 $V=\mathbb{C}^3$ 且

$$R_x=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}.$$

设 T 是矩阵为

$$B=\begin{bmatrix}2&1&0\\0&0&0\\0&0&0\end{bmatrix}$$

327 的线性算子．则$\tilde{T}$的矩阵是

$$\tilde{B}=\frac{1}{3}(IBI+R_x^{-1}BR_x+R_x^{-2}BR_x^2)$$

$$=\frac{1}{3}(B+R_x^2BR_x+R_xBR_x^2)=\frac{1}{3}\begin{bmatrix}2&1&0\\0&2&1\\1&0&2\end{bmatrix}.$$

或者，设 T 是矩阵为对应于对换 $y=(\mathbf{1}, \mathbf{2})$的置换矩阵的线性算子．群上的平均是三个对换的和：$(y+x^{-1}yx+x^{-2}yx)/3=(y+xy+x^2y)/3$．在这种情形下，

$$P=\frac{1}{3}\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\quad 而\quad \tilde{P}=\frac{1}{3}\begin{bmatrix}1&1&1\\1&1&1\\1&1&1\end{bmatrix}.$$

注意如前面所指出的[见(9.4)]，虽然原来的矩阵 P 和 B 不与 R_x 可交换，但$\tilde{B}$和$\tilde{P}$与 R_x 是可交换的．

我们将证明正交关系，即定理(5.9a)．在第六节已看到公式(5.10)是这些关系的一个结果．

设 χ，χ'是两个互不同构的既约特征标，对应于 G 在 V，V'上的表示 ρ，ρ'．利用法则 $\chi'(g^{-1})=\overline{\chi'(g)}$，可以将要证明的正交性$\langle\chi', \chi\rangle=0$ 重新写作

【9.11】
$$\frac{1}{N}\sum_g\chi'(g^{-1})\chi(g)=0.$$

现在舒尔引理断言每个 G-不变线性变换 $V\longrightarrow V'$为零，特别地，由对任意线性变换 T 取平均得到的线性变换$\tilde{T}$为零．把公式(9.9)考虑进来，这证明了下面的引理：

【9.12】引理 设 R，R'是 G 的互不同构的既约表示．则对每个适当形状的矩阵 A，

$$\sum_g R'_{g^{-1}}AR_g=0.$$

首先验证 ρ 和 ρ'为一维时的正交关系．在这种情形中，$R_{g'}$，R'_g是 1×1 矩阵，即为标量，而 $\chi(g)=R_g$．如果令 $A=1$，则除掉因子$\frac{1}{N}$，(9.12)变为(9.11)，这就完成了验证．

引理(9.12)也蕴涵了高维正交性，但需要一些计算．我们像在第四章第七节中那样，用

$(M)_{ij}$表示矩阵M的元素．则$\chi(g)=\text{trace}R_g=\sum_i(R_g)_{ii}$．于是$\langle\chi',\chi\rangle$展开为

【9.13】 $$\langle\chi',\chi\rangle=\frac{1}{N}\sum_g\sum_{i,j}(R'_{g^{-1}})_{ii}(R_g)_{jj}.$$

可以把和的顺序调过来．因而要证$\langle\chi',\chi\rangle=0$，只需证明对所有$i$，$j$，有 328

【9.14】 $$\sum_g(R'_{g^{-1}})_{ii}(R_g)_{jj}=0.$$

下面引理的证明是初等的：

【9.15】引理 设M，N是矩阵并设$P=Me_{\alpha\beta}N$，其中$e_{\alpha\beta}$是适当大小的矩阵单位．则P的元素是$(P)_{ij}=(M)_{i\alpha}(N)_{\beta j}$．

在引理(9.12)中用e_{ij}代替A并应用引理(9.15)，得到

$$0=(0)_{ij}=\sum_g(R'_{g^{-1}}e_{ij}R_g)_{jj}=\sum_g(R'_{g^{-1}})_{ii}(R_g)_{jj},$$

这正是所需证明的．它表明如果χ，χ'是互不同构的既约表示的特征标，则$\langle\chi',\chi\rangle=0$．

其次，假设$\chi=\chi'$．我们要证明$\langle\chi,\chi'\rangle=1$．这时如(9.9)一样取$A$的平均不会得零，但根据舒尔引理，它给出一个标量矩阵：

【9.16】 $$\frac{1}{N}\sum_g R_{g^{-1}}AR_g=\widetilde{A}=aI.$$

由命题(9.10)，$\text{trace}A=\text{trace}\,\widetilde{A}$，而且$\text{trace}\,\widetilde{A}=da$，其中$d=\dim\rho$．于是

【9.17】 $$a=\text{trace}A/d.$$

在(9.16)中取$A=e_{ij}$并再次应用引理(9.15)得到

【9.18】 $$(aI)_{ij}=\frac{1}{N}\sum_g(R_{g^{-1}}AR_g)_{ij}=\frac{1}{N}\sum_g(R_{g^{-1}})_{ii}(R_g)_{jj},$$

其中$a=(\text{trace}e_{ij})/d$．等式(9.18)的左边当$i\neq j$时为零而当$i=j$时等于$\frac{1}{d}$．这表明(9.13)中$i\neq j$的项为零，并且

$$\langle\chi,\chi\rangle=\frac{1}{N}\sum_g\sum_i(R_{g^{-1}})_{ii}(R_g)_{ii}=\sum_i\left[\frac{1}{N}\sum_g(R_{g^{-1}})_{ii}(R_g)_{ii}\right]=\sum_i\frac{1}{d}=1.$$

这就完成了既约特征标χ_1，χ_2，…是标准正交的证明．

我们仍需要证明既约特征标的个数等于共轭类的个数，或等价地，既约特征标张成类函数空间$\mathscr{C}$．设它们张成的子空间为$\mathcal{H}$．于是[第七章(2.7)]$\mathscr{C}=\mathcal{H}\oplus\mathcal{H}^{\perp}$．因此必须证明$\mathcal{H}^{\perp}=0$，或与每个特征标正交的类函数$\phi$为零．

假设给定类函数ϕ．于是ϕ是G上在共轭类上为常值的一个复值函数．设χ是一个表示ρ的特征标，考虑由

【9.19】 $$T=\frac{1}{N}\sum_g\overline{\phi(g)}\rho_g$$

定义的线性算子T：$V\longrightarrow V$．其迹为 329

【9.20】
$$\operatorname{trace}T=\frac{1}{N}\sum_g\overline{\phi(g)}\chi(g)=\langle\phi,\chi\rangle=0,$$

这是因为 ϕ 与 χ 是正交的.

【9.21】引理　(9.19)定义的算子 T 是 G 不变的.

证明　我们需要证明(9.2)对每一个 $h\in G$ 有 $\rho_h\circ T=T\circ\rho_h$，或 $T=\rho_h^{-1}\circ T\circ\rho_h$. 设 $g''=h^{-1}gh$. 则当 g 取遍群 G 时，g'' 也取遍 G，当然 $\rho_{h^{-1}}\rho_g\rho_h=\rho_{g''}$. 因为 ϕ 是类函数，$\phi(g)=\phi(g'')$. 因而有

$$\rho_h^{-1}T\rho_h=\frac{1}{N}\sum_g\overline{\phi(g)}\rho_h^{-1}\rho_g\rho_h$$
$$=\frac{1}{N}\sum_{g''}\overline{\phi(g'')}\rho_{g''}=T,$$

这正是要证的. ■

如果 ρ 是既约的，则可以使用舒尔引理(9.6b)得到 $T=cI$. 因为 $\operatorname{trace}T=0$(9.20)，可得 $T=0$. 任意表示 ρ 是既约表示的直和，且(9.19)与直和相容. 因而在每一情形都有 $T=0$.

将此用于 $\rho=\rho^{\text{reg}}$ 是正则表示的情形. 向量空间为 $V(G)$. 我们计算 $T(1)$，其中 1 表示 G 的单位元. 由正则表示的定义，$\rho_g(1)=g$. 于是

【9.22】
$$0=T(1)=\frac{1}{N}\sum_g\overline{\phi(g)}\rho_g(1)=\frac{1}{N}\sum_g\overline{\phi(g)}g.$$

由于 G 的元素是 $V=V(G)$ 的基，这证明了对所有 g 有 $\overline{\phi(g)}=0$，于是 $\phi=0$.

第十节　群 SU_2 的表示

一旦找到一个平移不变的(哈尔)测度 dg，第六节和第九节所做的大部分工作都可原封不动地搬到紧群 G 的连续表示上来. 只需把群上的求和换成积分即可. 然而如果 G 不是有限的，就会有无限多个既约表示.

当我们说到紧群的表示时，总是指一个到 $GL(V)$ 的连续同态，其中 V 是一个有限维的复向量空间. 这样 ρ 的特征标是 G 上的连续复值函数，它在每个共轭类上都为常数.（它是类函数.）

例如，恒等映射是 SU_2 的二维表示. 其特征标是 2×2 矩阵的通常的迹. 我们将称之为 SU_2 的标准表示. SU_2 的共轭类为具有给定迹 $2c$ 的矩阵的集合. 它们对应于 3-球面 SU_2 的纬 $\{x_1=c\}$[第八章(2.8)]. 由此，SU_2 的一个类函数仅依赖于 x_1. 因而这样的函数可认为是区间 $[-1,1]$上的连续函数. 使用第八章(2.5)的记号，SU_2 的标准表示的特征标为

$$\chi(P)=\operatorname{trace}P=a+\bar{a}=2x_1.$$

用 $|G|$ 表示紧群关于测度 dg 的体积：

【10.1】
$$|G|=\int_G 1dg.$$

于是用

【10.2】
$$\langle \chi,\chi' \rangle = \frac{1}{|G|}\int_G \overline{\chi(g)}\chi'(g)\mathrm{d}g$$
代替(5.8)的埃尔米特型．用这个定义，正交性关系成立．下面对紧群的拓广的证明与对有限群情形的证明是一样的．

【10.3】定理

(a) 紧群 G 的每一个有限维表示是既约表示的直和．

(b) 舒尔引理：设 ρ，ρ' 是既约表示，并设 $T: V \longrightarrow V'$ 是一个 G-不变的线性变换．则或者 T 是同构，或者 $T=0$．如果 $\rho=\rho'$，则 T 是一个标量的乘积．

(c) 既约表示的特征标关于型(10.2)是正交的．

(d) 如果两个表示的特征标相等，则这两个表示同构．

(e) 特征标 χ 具有性质 $\langle\chi, \chi'\rangle=1$ 当且仅当 ρ 是既约的．

(f) 如果 G 是阿贝尔的，则每个既约表示是一维的．

然而定理(5.9)的其他部分不能直接搬过去．理论上最有意义的变化在第六节．如果 G 是连通的，它不能在一个有限集上连续且非平凡地作用，因而有限维表示不能由一个在集合上的作用得到．特别是正则表示不是有限维的．需要用解析方法拓广理论的这一部分．

由于对群 U_1 和 SU_2 容易找到哈尔测度，所以我们会考虑为它们证明的(10.3)的全部．

容易描述圆群 U_1 的表示，但对理解任意的紧群它们是最基本的．交替使用加法和乘法记号将是方便的：

【10.4】
$$SO_2(\mathbb{R}) \xrightarrow{\sim} U_1$$
$$(\text{转过}\,\theta) \rightsquigarrow e^{i\theta} = \alpha.$$

331

【10.5】定理　U_1 的既约表示是 n 次指数映射：
$$U_1 \xrightarrow{\text{“}n\text{”}} U_1,$$
使 $\alpha \rightsquigarrow \alpha^n$ 或 $\theta \rightsquigarrow n\theta$．对每个整数 n 存在一个这样的表示．

证明　由(10.3f)，既约表示都是一维的，且由(3.5)，它们与酉表示共轭．由于 $GL_1=\mathbb{C}^\times$ 是阿贝尔的，因此共轭是平凡的，于是一个一维矩阵表示自动是酉的．因此 U_1 是由 U_1 到它自身的连续同态．我们只需证明这样的同态是 n 次指数映射．

【10.6】引理　连续同态 $\psi: \mathbb{R}^+ \longrightarrow \mathbb{R}^+$ 是标量乘积：存在 $c\in\mathbb{R}$ 使得 $\psi(x)=cx$．

证明　设 $\psi: \mathbb{R}^+ \longrightarrow \mathbb{R}^+$ 为连续同态．我们将证明对所有 x 有 $\psi(x)=x\psi(1)$．这将证明 ψ 是用 $c=\psi(1)$ 作的乘法．

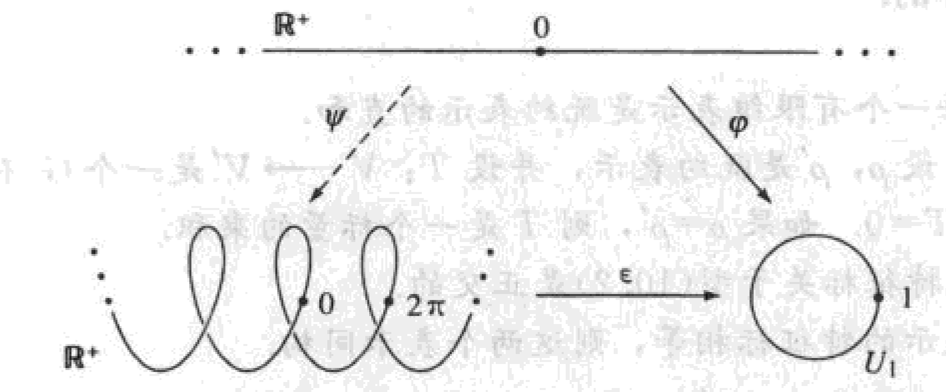
由于 ψ 是同态，对任意实数 r 及任意非负整数 n，$\psi(nr)=\psi(r+\cdots+r)=n\psi(r)$．特别地，$\psi(n)=n\psi(1)$．而且 $\psi(-n)=-\psi(n)=-n\psi(1)$．因此对每个整数 n 有 $\psi(n)=n\psi(1)$．其次设 $r=\frac{m}{n}$ 为有理数．则 $n\psi(r)=\psi(nr)=\psi(m)=m\psi(1)$．除于 n 得到对每个有理数 r 有 $\psi(r)=r\psi(1)$．由于有理数在 $\mathbb{R}$ 中稠密且 ψ 连续，因此对所有 x 有 $\psi(x)=cx$．■

【10.7】引理　存在 $c\in\mathbb{R}$，使得连续同态 $\varphi:\mathbb{R}^+ \longrightarrow U_1$ 具有 $\varphi(x)=e^{icx}$ 的形式．

证明　如果 φ 可微，这可用第八章第五节的指数映射来证明．我们现在对任意连续映射来证明．考虑由 $\varepsilon(x)=e^{ix}$ 定义的指数同态 ε：$\mathbb{R}^+ \longrightarrow U_1$．这个同态将实直线以 2π 为周期绕到单位圆上

[见图(10.8)]．对使得 $\varphi(0)=1$ 的任意连续函数 $\varphi:\mathbb{R}^+\longrightarrow U_1$，存在这个函数到实直线上唯一的连续提升 ψ，满足 $\psi(0)=0$．换言之，可以找到唯一的连续函数 ψ：$\mathbb{R}\longrightarrow\mathbb{R}$ 使得 $\psi(0)=1$，且对所有 x 有 $\varphi(x)=\varepsilon(\psi(x))$．提升的构造从定义 $\psi(0)=1$ 开始，然后依次将 ψ 在一个个小区间上拓广．

【10.8】图



我的断言如果 φ 是同态，则其提升 ψ 也是同态．如果证明了这一点，则由(10.6)可以得到对某个 c，有 $\psi(x)=cx$，因而 $\varphi(x)=e^{icx}$，这正是所要证明的．

关系 $\varphi(x+y)=\varphi(x)\varphi(y)$ 蕴涵 $\varepsilon(\psi(x+y)-\psi(x)-\psi(y))=1$．因而对某个连续地依赖于 x 和 y 的整数 m 有 $\psi(x+y)-\psi(x)\psi(y)=2\pi m$．由于变化是连续的，$m$ 必为常数，且当取 $x=y=0$ 时得出 $m=0$．于是 ψ 为同态，这正是所断言的．■

现在来完成定理(10.5)的证明，设 ρ：$U_1\longrightarrow U_1$ 是一个连续同态．则 $\varphi=\rho\circ\varepsilon$：$\mathbb{R}^+\longrightarrow$ 332 U_1 亦是连续同态，于是由(10.7)，$\varphi(x)=e^{icx}$．此外，$\varphi(2\pi)=\rho(1)$，这一点成立当且仅当 c 为整数，设为 n．于是 $\rho(e^{ix})=e^{inx}=(e^{ix})^n$．

现在我们检查群 SU_2 的表示．这里也存在一个自然出现的既约表示的无限簇，且它们最终构成一个完全的列表．设 V_n 是变量 u，v 的 n 次齐次多项式的集合．这样的多项式具有

【10.9】
$$f(u,v)=x_0u^n+x_1u^{n-1}v+\cdots+x_nv^n$$

的形式，其中系数 x_i 为复数．显然，V_n 是一个 $n+1$ 维向量空间，基为(u^n，$u^{n-1}v$，…，v^n)．群 $G=GL_2$ 以下列方式在 V_n 上作用：设 $P\in GL_2$，比如设

$$P=\begin{bmatrix}a & b\\ c & d\end{bmatrix}.$$

设 P 在 V_1 的基(u，v)上按通常方式作用：

$$(u',v')=(u,v)P=(au+cv,bu+dv);$$

用规则

【10.10】
$$u^iv^j \rightsquigarrow u'^iv'^j \text{ 及}$$
$$f(u,v)\rightsquigarrow x_0u'^n+x_1u'^{n-1}v'+\cdots+x_nv'^n$$

定义 ρ_{n_P}．这是一个表示

【10.11】
$$\rho_n:G\longrightarrow GL(V_n)\approx GL_{n+1}.$$

平凡表示为 ρ_0 而标准表示为 ρ_1．

例如，ρ_{2_P} 的矩阵为

【10.12】
$$R_{2_P}=\begin{bmatrix}a^2 & ab & b^2\\ 2ac & ad+bc & 2bd\\ c^2 & cd & d^2\end{bmatrix}.$$

其中第一列是 $\rho_{2_P}(u^2)=(au+cv)^2=a^2u^2+2acuv+c^2v^2$ 的坐标向量，等等. [333]

【10.13】定理 通过将(10.11)限制在子群 SU_2 上得到的表示 $\rho_n(n=0, 1, 2, \cdots)$ 是 SU_2 的既约表示.

证明 考虑 SU_2 的对角矩阵

【10.14】
$$\begin{bmatrix}\alpha & \\ & \bar{\alpha}\end{bmatrix}$$

的子群 T，其中 $\alpha=e^{i\theta}$. 这个群同构于 U_1. 任意酉矩阵 P 的共轭类包含两个对角矩阵，即

$$\begin{bmatrix}\lambda & \\ & \bar{\lambda}\end{bmatrix}\text{和}\begin{bmatrix}\bar{\lambda} & \\ & \lambda\end{bmatrix},$$

其中 λ，$\bar{\lambda}$ 是 P 的特征值[第七章(7.4)]. 只有当 $\lambda=\pm1$ 时它们才相等. 于是除了 $\{I\}$ 和 $\{-I\}$ 外每个共轭类与 T 的交为两个矩阵.

【10.15】命题

(a) SU_2 上的类函数由它在子群 T 上的限制确定.

(b) 类函数 φ 在 T 上的限制是一个偶函数，这是指

$$\varphi(\alpha)=\varphi(\bar{\alpha}) \text{ 或 } \varphi(\theta)=\varphi(-\theta).$$

其次，SU_2 的任意表示 ρ 限制到一个子群 T 上的表示，而 T 与 U_1 同构. SU_2 的一个既约表示在 T 上的限制通常是可约的，但它可以分解为 T 上的既约表示的直和. 因而特征标 χ 在 T 上的限制给出 U_1 上既约特征标的和. 定理(10.5)告诉我们什么是 T 的既约特征标：它们是 n 次幂 $e^{in\theta}$，其中 $n\in\mathbb{Z}$. 从而得到：

【10.16】命题 SU_2 的特征标 χ 在 T 上的限制是指数函数 $e^{in\theta}$ 的有限和.

我们计算 ρ_n 的特征标 χ_n(10.11)在 T 上的限制. 矩阵(10.14)在单项式上的作用为

$$u^iv^j \rightsquigarrow (\alpha^iu^i)(\bar{\alpha}^jv^j)=\alpha^{i-j}u^iv^j.$$

因而它在基$(u^n, u^{n-1}v, \cdots, v^n)$上的作用的矩阵是对角矩阵

$$\begin{bmatrix}\alpha^n & & & \\ & \alpha^{n-2} & & \\ & & \ddots & \\ & & & \ddots \\ & & & & \alpha^{-n}\end{bmatrix},$$

而特征标的值为 [334]

【10.17】
$$\chi_n(\alpha)=\alpha^n+\alpha^{n-2}+\cdots+\alpha^{-n}=e^{in\theta}+e^{i(n-2)\theta}+\cdots+e^{-in\theta},$$

或

【10.18】
$$\begin{aligned}\chi_0&=1\\ \chi_1&=2\cos\theta=e^{i\theta}+e^{-i\theta}\\ \chi_2&=1+2\cos2\theta=e^{2i\theta}+1+e^{-2i\theta}\\ \chi_3&=2\cos3\theta+2\cos\theta\\ &\vdots\end{aligned}$$

现在设 χ' 为 SU_2 上的任意一个既约特征标．它在 T 上的限制是偶的(10.15b)并且是指数 $e^{in\theta}$ 的和(10.16)．要成为偶的，$e^{in\theta}$ 和 $e^{-in\theta}$ 必须以同样的系数出现，因此特征标是函数 $\cos n\theta=\frac{1}{2}(e^{in\theta}+e^{-in\theta})$ 的线性组合．函数(10.17)构成由 $\{\cos n\theta\}$ 张成的向量空间的一个基．因而

【10.19】
$$\chi'=\sum_i r_i\chi_i,$$

其中 r_i 为有理数．我们已经知道这在 T 上是成立的，但由(10.15a)，它在整个 SU_2 上也成立．去分母并将负项移到(10.19)的左边得到形如

【10.20】
$$m\chi'+\sum_j n_j\chi_j=\sum_k n_k\chi_k$$

的关系，其中 n_j，n_k 为正整数且指标集 $\{j\}$，$\{k\}$ 互不相交．这个关系蕴涵

$$m\rho'\oplus\sum_j n_j\rho_j=\sum_k n_k\rho_k.$$

因而 ρ' 是表示 ρ_k 中的一个．这完成了定理(10.13)的证明． ■

我们将明显的推广留给读者.

Israel Herstein

练　习

第一节　群表示的定义

335

1. 设 ρ 是群 G 的一个表示．证明 $\det\rho$ 是一个一维表示．
2. 假设 G 是一个群，具有一个由对角矩阵给出的忠实表示．证明 G 是阿贝尔群．
3. 证明由 $p \rightsquigarrow \operatorname{sign}p$ 定义的法则 $S_n\longrightarrow\mathbb{R}^\times$ 是对称群的一维表示．
4. 证明对称群 S_5 仅有的一维表示是由对所有 g，$\rho(g)=1$ 定义的平凡表示和符号表示．
5. (a) 选择 $\mathbb{R}^3$ 适当的基，用旋转具体写出正八面体群 O 的标准表示．
   (b) 对二面体群 D_n 做同样的练习．
   *(c) 对正二十面体群 I 做同样的练习．
6. 当 SO_2 的一个旋转由其角度表示时，证明规则 $\sigma(\theta)=\begin{bmatrix}\alpha & \alpha^2-\alpha\\ 0 & \alpha^2\end{bmatrix}$ 是 SO_2 的一个表示，其中 $\alpha=e^{i\theta}$．
7. 设 H 是群 G 的一个指数为 2 的子群，并设 ρ：$G\longrightarrow GL(V)$ 是一个表示．当 $g\in H$ 时 $\rho'(g)=\rho(g)$ 而当 $g\notin H$ 时 $\rho'(g)=-\rho(g)$，利用这一规则定义 ρ'：$G\longrightarrow GL(V)$．证明 ρ' 是 G 的一个表示．
8. 证明每一有限群 G 在有限维复向量空间上有一个忠实表示．
9. 设 N 是群 G 的一个正规子群．将 G/N 的表示与 G 的表示联系起来．
10. 选择 $\mathbb{R}^3$ 的三个轴使之过中心在原点的正四面体的顶点．(这不是一个正交坐标系)．求第四个顶点的坐标，并具体写出正四面体群 T 在这个坐标系下的矩阵表示．

第二节　G-不变型与酉表示

1. (a) 验证型 X^*BY(2.10)是 G-不变的．
   (b) 求这个型的标准正交基，并求基变换矩阵 P．验证 PAP^{-1} 是酉的．
2. 证明(2.2)的实类似：设 R：$G\longrightarrow GL_n(\mathbb{R})$ 是有限群 G 的表示．存在 $P\in GL_n(\mathbb{R})$ 使得对每个 $g\in G$，

PR_gP^{-1}是正交的.

3. 设ρ：$G \longrightarrow GL_2(\mathbb{R})$是有限群$G$通过行列式为1的实$2\times2$矩阵的忠实表示. 证明$G$是循环群.
4. 求所有具有实二维忠实表示的有限群.
5. 描述具有行列式为1的三维忠实实表示的有限群G.
6. 设V是埃尔米特向量空间. 证明V上的酉算子构成$GL(V)$的子群$U(V)$，并且V上的表示ρ的象属于$U(V)$当且仅当型$\langle,\rangle$是G-不变的.
7. 设$\langle,\rangle$是向量空间V上非退化的斜对称型，并设ρ是有限群G在V上的表示.

   (a) 证明平均过程(2.7)产生一个V上的G-不变的斜对称型.

   (b) 这是否证明了GL_{2n}的每一个有限子群与SP_{2n}的一个子群共轭?

336

8. (a) 设R是D_3的标准二维表示，其中三角形的位置使得x-轴是一条反射的直线. 用基$x'=x$及$y'=x+y$重新写出这个表示.

   (b) 利用平均过程由(x', y')-坐标上的点积得到一个G-不变型.

第三节 紧群

1. 证明$\mathrm{d}x/x$是乘法群$\mathbb{R}^\times$的一个哈尔测度.
2. (a) 设$P=\begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}$为一个$2\times2$变量矩阵，并设$\mathrm{d}V=\mathrm{d}p_{11}\mathrm{d}p_{12}\mathrm{d}p_{21}\mathrm{d}p_{22}$表示$\mathbb{R}^{2\times2}$中通常的体积型. 证明$(\det P)^{-2}\mathrm{d}V$是$GL_2(\mathbb{R})$的一个哈尔测度.

   (b) 推广(a)的结果.

*3. 证明3-球面上的型$\dfrac{\mathrm{d}x_2\mathrm{d}x_3\mathrm{d}x_4}{x_1}$定义$SU_2$的一个哈尔测度. 在$x_1=0$点用什么来代替这个表达式?

4. 取$\mathbb{R}^2$上由

$$\sigma(\theta)=\begin{bmatrix} \alpha & \alpha^2-\alpha \\ 0 & \alpha^2 \end{bmatrix},\quad \alpha=\mathrm{e}^{i\theta}$$

给出的SO_2的复表示，通过对$\mathbb{R}^2$上的埃尔米特型取平均将它化为一个酉表示.

第四节 G-不变子空间与既约表示

1. 证明正四面体群T的标准三维表示作为复表示是既约的.
2. 求循环群C_n的所有既约表示.
3. 求二十面体群I的不忠实的表示.
4. 设ρ是有限群G在一个向量空间V上的表示并设$v\in V$.

   (a) 证明在G上平均gv给出一个在G作用下不变的向量$\bar{v}\in V$.

   (b) 如果ρ是既约表示，关于这个向量你有什么结论?

5. 设$H\subset G$是一个子群，设ρ是群G在V上的表示，并设$v\in V$. 令$w=\sum\limits_{h\in H}hv$. 关于w的G-轨道的阶你有什么结论?
6. 考虑二面体群D_n作为正n-边形的对称的标准二维表示. 当n取什么值时它作为复表示是既约的?

*7. 设G是如第五章(3.6)所表出的二面体群D_3.

   (a) 设ρ为一个既约的二维酉表示. 证明存在V的标准正交基使得$R_y=\begin{bmatrix} 1 & \\ & -1 \end{bmatrix}$.

   (b) 假设R_y如上. 利用定义关系$yx=x^2y$，$x^3=1$来确定R_x的可能性.

   (c) 证明G的所有既约二维表示都同构.

   (d) 设ρ是G的任意表示，设$v\in V$是算子ρ_x的一个特征向量. 证明v含于一个维数$\leqslant2$的G-不变子空间

W 中.

337 (e) 确定 G 的所有既约表示.

第五节 特征标

1. 推论(5.11)描述了类函数空间的一个基. 请给出另一个基.
2. 求出循环群 C_n 通过旋转给出的标准二维旋转表示分解成为既约表示的分解.
3. 证明或推翻: 设 χ 是有限群 G 的特征标, 定义 $\bar{\chi}(g)=\overline{\chi(g)}$. 则 $\bar{\chi}$ 亦是 G 的特征标.
4. 求正方体的旋转群 O、四元数群以及二面体群 D_4, D_5, D_6 的既约表示的维数.
5. 描述如何通过调整一个特征标表的元素作出一个酉矩阵.
6. 比较四元数群与二面体群 D_4 的特征标表.
7. 求 D_6 的特征标表.
8. (a) 求群 C_5 和 D_5 的特征标表.

   (b) 把 D_5 的每个既约特征标的限制分解为 C_5 的既约特征标.
9. (a) 设 ρ 为一个 d 维表示, 特征标为 χ. 证明 ρ 的核是使 $\chi(g)=d$ 的群元素的集合.

   (b) 证明如果 G 有一个真的正规子群, 则存在表示 ρ 使其核 $\ker\rho$ 为一个真的正规子群.

*10. 设 χ 是 d 维表示 ρ 的特征标. 证明对所有 $g\in G$ 有 $|\chi(g)|\leqslant d$, 且如果 $|\chi(g)|=d$, 则对某个单位根 ζ, 有 $\rho(g)=\zeta I$.

11. 设 $G'=G/N$ 是有限群 G 的商群, 并设 ρ' 是 G' 的既约表示. 用直接证明及利用定理(5.9)两种方式证明: 由 ρ' 定义的 G 的表示是既约的.
12. 求下列特征标表中缺失的行:

	(1)	(3)	(6)	(6)	(8)
	1	a	b	c	d
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	3	-1	1	-1	0
χ_4	3	-1	-1	1	0

13. 下面的表是一个有限群的特征标表的一部分, 其中 $\zeta=\frac{1}{2}(-1+\sqrt{3}\mathrm{i})$ 而 $\gamma=\frac{1}{2}(-1+\sqrt{7}\mathrm{i})$. 共轭类都在这里.

	(1)	(3)	(3)	(7)	(7)
χ_1	1	1	1	ζ	$\bar{\zeta}$
χ_2	3	γ	$\bar{\gamma}$	0	0
χ_3	3	$\bar{\gamma}$	γ	0	0

   (a) 确定群的阶与既约表示的个数和维数.

   (b) 确定其余的特征标.

338 (c) 用生成元和关系描述这个群.

*14. 用特征标表描述群 G 的换位子子群.

*15. 下面是一个特征标表的一部分, 缺少一个共轭类.

	(1)	(1)	(2)	(2)	(3)
	1	u	v	w	x
χ_1	1	1	1	1	1
χ_2	1	1	1	1	-1
χ_3	1	-1	1	-1	i
χ_4	1	-1	1	-1	$-$i
χ_5	2	-2	-1	-1	0

(a) 将特征标表补充完整.

(b) 证明 u 的阶为 2，x 的阶为 4，w 的阶为 6，而 v 的阶为 3. 确定缺失的共轭类中元素的阶.

(c) 证明 v 生成一个正规子群.

(d) 描述这个群.

*16. (a) 求下面的特征标表缺失的行.

(b) 证明具有这个特征标表的群 G 有一个 10 阶的子群 H，并将这个子群描述为共轭类的并.

(c) 确定 H 是 C_{10} 还是 D_5.

(d) 确定 G 的换位子子群.

(e) 确定 G 的所有正规子群.

(f) 确定元素 a，b，c，d 的阶.

(g) 确定这个群的西罗 2-子群和西罗 5-子群的个数.

	(1)	(4)	(5)	(5)	(5)
	1	a	b	c	d
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	1	1	$-$i	i	-1
χ_4	1	1	i	$-$i	-1

*17. 在下列特征标表中，$\zeta=\frac{1}{2}(-1+\sqrt{3}\mathrm{i})$.

	(1)	(6)	(7)	(7)	(7)	(7)	(7)
	1	a	b	c	d	e	f
χ_1	1	1	1	1	1	1	1
χ_2	1	1	1	ζ	$\bar{\zeta}$	ζ	$\bar{\zeta}$
χ_3	1	1	1	$\bar{\zeta}$	ζ	$\bar{\zeta}$	ζ
χ_4	1	1	-1	$-\zeta$	$-\bar{\zeta}$	ζ	$\bar{\zeta}$
χ_5	1	1	-1	$-\bar{\zeta}$	$-\zeta$	$\bar{\zeta}$	ζ
χ_6	1	1	-1	-1	-1	1	1
χ_7	6	-1	0	0	0	0	0

(a) 证明 G 有一个同构于 D_7 的正规子群 N，并确定 G/N 的结构.

(b) 将每个特征标在 N 的限制分解为既约 N-特征标.

(c) 对 $p=2$，3，7 确定西罗 p-子群的个数.

(d) 确定代表元素 c，d，e，f 的阶.

339

第六节　置换表示与正则表示

1. 验证(6.4)和(6.5)的特征标的值.
2. 利用正交关系分解正四面体群的正则表示的特征标.
3. 证明任意阶为 $N>1$ 的群 G 的既约表示的维数最多是 $N-1$.
4. 求 12 阶非阿贝尔群的特征标表.
5. 将 C_3 的正则表示分解为既约实表示.
6. 证明推论(6.8).
7. 设 ρ 是与 D_3 的由共轭在其自身上的作用相伴的置换表示. 将 ρ 的特征标分解为既约特征标.
8. 设 S 是一个 G-集合并设 ρ 是 G 在空间 $V(S)$ 上的置换表示. 证明 S 的轨道分解导出 ρ 的一个直和分解.
9. 证明对称群 S_n 通过置换矩阵给出的标准表示是一个平凡表示和一个既约表示的和.

*10. 设 H 是有限群 G 的一个子群. 给定 G 的一个既约表示 ρ, 可以将其在 H 上的限制分解为既约 H-表示. 证明 H 的每一个既约表示可以用这种方式得到.

第七节　正二十面体群的表示

1. 计算 I 的特征标 χ_2, χ_4, χ_5, 并利用正交关系确定剩下的特征标 χ_3.
2. 将正二十面体群在面、边和顶点的集合上的表示分解成既约表示.
3. 群 S_5 通过共轭在其子群 A_5 上作用. 这个作用如何作用在 A_5 的既约表示的集合上?

*4. 推导出一个通过检视其特征标表而验证一个群为单群的算法.

5. 利用正二十面体群的特征标表证明它是单群.
6. 设 H 是群 G 的一个指标为 2 的子群, 并设 σ: $H \longrightarrow GL(V)$ 为一个表示. 设 a 是 G 中不属于 H 的元素. 用规则 $\sigma'(h)=\sigma(a^{-1}ha)$ 定义一个共轭表示 σ': $H \longrightarrow GL(V)$.
   (a) 证明 σ' 是 H 的一个表示.
   (b) 证明如果 σ 是 G 的一个表示在 H 的限制, 则 σ' 与 σ 同构.
   (c) 证明如果 b 是 G 中另一个不属于 H 的元素, 则表示 $\sigma''(h)=\sigma(b^{-1}hb)$ 与 σ' 同构.

340

7. (a) 选择一个坐标系并具体写出正八面体群 O 的标准三维矩阵表示.
   (b) 确定 O 的五个共轭类, 并求其既约表示的阶.
   (c) 群 O 在这些集合上作用:
      i. 正方体的六个面
      ii. 三对对面
      iii. 八个顶点
      iv. 四对对顶
      v. 六对对边
      vi. 两个内接正四面体
   将 O 的既约表示等同于这些表示的直和项, 并计算 O 的特征标表. 验证正交关系.
   (d) 将(c)中的每个表示分解为既约表示.
   (e) 利用特征标表求 O 的所有正规子群.
8. (a) 正二十面体群 I 包含一个子群 T, 也就是其中一个立方体的稳定子[第六章(6.7)]. 分解 I 的既约特征标在 T 的限制.
   (b) 像(a)一样对 I 的子群 D_5 做同样的练习.
9. 下面是群 $G=PSL_2(\mathbb{F}_7)$ 的特征标表, 其中 $\gamma=\frac{1}{2}(-1+\sqrt{7}\mathrm{i})$, $\gamma'=\frac{1}{2}(-1-\sqrt{7}\mathrm{i})$.

	(1)	(21)	(24)	(24)	(42)	(56)
	1	a	b	c	d	e
χ_1	1	1	1	1	1	1
χ_2	3	−1	γ	γ'	1	0
χ_3	3	−1	γ'	γ	1	0
χ_4	6	2	−1	−1	0	0
χ_5	7	−1	0	0	−1	1
χ_6	8	0	1	1	0	−1

(a) 用它给出该群是单群的两个不同的证明.

(b) 尽可能多地确定元素

$$\begin{bmatrix}1 & 1\\ & 1\end{bmatrix},\ \begin{bmatrix}2 & \\ & 4\end{bmatrix}$$

的共轭类并求出代表剩下的共轭类的矩阵.

(c) G 在 $F^2(F=\mathbb{F}_7)$ 的一维子空间的集合上作用. 将相伴的特征标分解为既约特征标.

第八节 一维表示

1. 证明群 G 的阿贝尔特征标构成一个群.
2. 对克莱因四元群和四元数群确定其特征标群.
3. 设 A, B 都是某次幂矩阵为单位矩阵的矩阵且 A 与 B 交换. 证明存在可逆矩阵 P 使得 PAP^{-1} 和 PBP^{-1} 都是对角矩阵.
4. 设 G 是有限阿贝尔群. 证明其特征标群的阶等于 G 的阶.

341

*5. 证明符号表示 $p \rightsquigarrow \operatorname{sign} p$ 及平凡表示是对称群 S_n 仅有的一维表示.

6. 设 G 是 n 阶循环群, 由一个元素 x 生成, 并设 $\zeta=e^{2\pi i/n}$.

   (a) 证明其既约表示为 ρ_0, …, ρ_{n-1}, 其中 ρ_k: $G \rightsquigarrow \mathbb{C}^\times$ 由 $\rho_k(x)=\zeta^k$ 定义.

   (b) 确定 G 的特征标群.

   (c) 对 G 具体验证正交关系.

7. (a) 设 $\varphi: G \longrightarrow G'$ 是阿贝尔群的同态. 定义一个其特征标群之间的诱导同态 $\hat{\varphi}$: $\hat{G}' \longleftarrow \hat{G}$.

   (b) 证明如果 φ 是单射, 则 $\hat{\varphi}$ 是满射, 反之亦然

第九节 舒尔引理和正交关系的证明

1. 设 ρ 是 G 的表示. 证明或推翻: 如果 V 上仅有的 G-不变算子是用标量乘, 则 ρ 是既约的.
2. 设 ρ 是 T 的标准三维表示, 并设 ρ' 是由 T 在四个顶点上作用得到的置换表示. 用平均法证明 ρ 是 ρ' 的一个直和项.
3. 设 $\rho=\rho'$ 是二面体群 D_3 的一个二维表示(4.6), 并设 $A=\begin{bmatrix}1 & 1\\ & \end{bmatrix}$. 用平均过程由 A 的左乘作出一个 G-不变的变换.
4. (a) 证明 $R_x=\begin{bmatrix}1 & 1 & -1\\ & & 1\\ 1 & & -1\end{bmatrix}$, $R_y=\begin{bmatrix} & -1 & -1\\ -1 & & 1\\ & & -1\end{bmatrix}$ 定义 D_3 的一个表示.

   (b) 可将(5.15)的表示 ρ_2 视为 1×1 矩阵表示. 设 T 是矩阵为 $(1, 0, 0)^t$ 的线性变换 $\mathbb{C}^1 \longrightarrow \mathbb{C}^3$. 使用 ρ_2 和 (a)中定义的表示 R, 应用平均方法由 T 作出一个 G-不变的线性变换.

(c) 用 ρ_1 和 ρ_3 代替 ρ_2 作(b).

(d) 将 R 具体分解为既约表示.

第十节 群 SU_2 的表示

1. 确定旋转群 SO_3 的既约表示.
2. 确定正交群 O_2 的既约表示.
3. 证明正交表示 $SU_2 \longrightarrow SO_3$ 是既约的，在(10.18)的列表中找出其特征标.
4. 证明函数(10.18)构成由 $\{\cos n\theta\}$ 张成的向量空间的基.
5. 如第八章第二节，左乘定义了 SU_2 在坐标为 x_1，x_2，x_3，x_4 的空间$\mathbb{R}^4$ 上的一个表示. 将与之相伴的复表示分解为既约表示.
6. (a) 通过切为三维切片计算半径为 r 的 4-球 $B^4=\{x_1^2+x_2^2+x_3^2+x_4^2+\leqslant r^2\}$的四维体积.

342

(b) 仍通过切片计算 3-球面 S^3 的三维体积. 建议先复习一下 2-球面面积的类似计算. 应该得到$\frac{\mathrm{d}}{\mathrm{d}r}$($B^4$ 的体积)=(S^3 的体积). 如果不对，再试一试.

*7. 通过在 S^3 上作积分证明 SU_2 的既约特征标(10.17)的正交性关系.

杂题

*1. 证明非素数阶的有限单群没有二维非平凡表示.

*2. 设 H 是有限群 G 的一个指标为 2 的子群，并设 a 是 G 中一个不属于 H 的元素，于是 aH 是 H 在 G 中的另一个陪集. 设 S：$H \longrightarrow GL_n$ 是 H 的一个矩阵表示. 定义 G 的一个称为诱导表示的表示 ind S：$G \longrightarrow GL_{2n}$如下：

$$(\text{ind } S)_h=\left[\begin{array}{c|c} S_h & \\ \hline & S_{a^{-1}ha}\end{array}\right],\quad (\text{ind } S)_{ah}=\left[\begin{array}{c|c} & S_{aha} \\ \hline S_h & \end{array}\right],$$

(a) 证明 ind S 是 G 的一个表示.

(b) 用 S 的特征标 χ_S 描述 ind S 的特征标 $\chi_{\text{ind } S}$.

(c) 如果 R：$G \longrightarrow GL_m$ 是 G 的一个表示，则可将其限制于 H. 将限制记为 res R：$H \longrightarrow GL_m$. 证明 res(ind S)$\approx S \oplus S'$，其中 S'是由 $S'_h=S_{a^{-1}ha}$定义的共轭表示.

(d) 证明弗罗贝尼乌斯互反律：$\langle \chi_{\text{ind } S}, \chi_R\rangle=\langle \chi_S, \chi_{\text{res } R}\rangle$.

(e) 用弗罗贝尼乌斯互反律证明如果 S 和 S'是互不同构的表示，则 G 的诱导表示 ind S 是既约的. 另一方面，若 $S\approx S'$，则诱导的表示 ind S 是两个既约表示 R，R'的和.

*3. 设 H 是群 G 的指标为 2 的子群，并设 R 是 G 的一个矩阵表示. 用 R'表示共轭表示，定义为如果 $g\in H$ 则 $R'_g=R_g$否则 $R'_g=-R_g$.

(a) 证明 R'同构于 R 当且仅当 $g\notin H$ 时 R 的特征标在陪集 gH 上恒等于零.

(b) 用弗罗贝尼乌斯互反律证明 ind(res R)$\approx R\oplus R'$.

(c) 证明如果 R 与 R'不同构，则 res R 为既约的，如果这两个表示同构，则 res R 为 H 的两个既约表示的和.

*4. 当(a) $n=3$，(b) $n=4$，(c) $n=5$ 时，用弗罗贝尼乌斯互反律从 A_n 的特征标表导出 S_n 的特征标表.

*5. 利用从 C_n 诱导的表示确定二面体群 D_n 的特征标表.

6. (a) 证明 SU_2 仅有的 2 阶元素是 $-I$.

(b) 考虑同态 φ:$SU_2 \longrightarrow SO_3$. 设 A 是 SU_2 中使得 $\varphi(A)=\bar{A}$并在 SO_3 中为有限阶$\bar{n}$的元素. 证明 A 的阶 n 为$\bar{n}$或 2 $\bar{n}$. 并且证明如果$\bar{n}$是偶数，则 $n=2\bar{n}$.

*7. 设 G 是 SU_2 的有限子群，并设$\bar{G}=\varphi(G)$，其中 $\varphi: SU_2 \longrightarrow SO_3$ 是正交表示(第八章第三节)．证明下面的结果．

(a) 如果 $|\bar{G}|$ 为偶的，则 $|G|=2|\bar{G}|$ 且 $G=\varphi^{-1}(\bar{G})$．

343

(b) 或者 $G=\varphi^{-1}(\bar{G})$，或者 G 是奇数阶循环群．

(c) 设 G 是 SU_2 的 n 阶循环子群．证明 G 与由$\begin{bmatrix}\zeta & \\ & \zeta^{-1}\end{bmatrix}$生成的子群共轭，其中 $\zeta=e^{2\pi i/n}$．

(d) 证明如果$\bar{G}$是群 D_2，则 G 是四元数群．确定四元数群 H 作为 SU_2 的子群关于$\mathbb{C}^2$ 适当的标准正交基的矩阵表示．

(e) 如果$\bar{G}=T$，证明 G 是不同构于对称群 S_4 的 24 阶群．

*8. 设 ρ 是有限群 G 的既约表示．正定 G-不变埃尔米特型的唯一性如何？

*9. 设 G 是 $GL_n(\mathbb{C})$的有限子群．证明如果 $\sum_g \operatorname{tr} g=0$，则 $\sum_g g=0$．

*10. 设 $\rho: G \longrightarrow GL(V)$为有限群 G 的一个二维表示，并假设对每个 $g \in G$，1 是 ρ_g 的一个特征值．证明 ρ 是两个一维表示的和．

*11. 设 $\rho: G \longrightarrow GL_n(\mathbb{C})$是有限群 G 的一个既约表示．给定 GL_n 的任意表示 $\sigma: GL_n \longrightarrow GL(V)$，可以将合成$\sigma \circ \rho$视为 G 的表示．

(a) 当 σ 是 GL_n 在 $n\times n$ 矩阵空间$\mathbb{C}^{n\times n}$的左乘时，确定以这种方式得到的表示的特征标．在此情形将 $\sigma \circ \rho$ 分解为既约表示．

(b) 当 σ 是在 $M_n(\mathbb{C})$上的共轭作用时求 $\sigma \circ \rho$ 的特征标．

344

第十章　环

请忘掉你在中学所学的一切，
因为你并没有学懂.

Edmund Landau

第一节　环的定义

整数构成环的概念的基本模型. 它们在加法、减法、乘法下封闭，但在除法下不封闭.

在给出环的抽象定义之前，我们通过考虑复数的子环先看一些例子. $\mathbb{C}$ 的一个子环是一个在加法、减法、乘法下封闭且包含 1 的子集. 这样任意子域[第三章(2.1)]都是子环. 另一个例子是高斯整数，它们是形如 $a+bi$(其中 a，b 是整数)的复数. 这个环记作

【1.1】
$$\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}.$$

高斯整数是复平面上方格的点.

可以从任意复数 α 入手构造与高斯整数环类似的子环 $\mathbb{Z}[\alpha]$. 我们把 $\mathbb{Z}[\alpha]$ 定义为 $\mathbb{C}$ 中包含 α 的最小子环，并称之为由 α 生成的子环. 不难描述这个环. 如果一个环包含 α，则由于它在乘法之下封闭，它包含 α 的所有正幂次. 而且它包含这些幂的和与差，还包含 1. 因而它包含可以写为 α 的整系数多项式的任意复数 β：

【1.2】
$$\beta=a_n\alpha^n+\cdots+a_1\alpha+a_0,\quad 其中\ a_i\in\mathbb{Z}.$$

345 换言之，所有这样的数的集合在加法、减法、乘法的作用下封闭，并且包含 1. 因而它是由 α 生成的子环. 但在大多数情形中 $\mathbb{Z}[\alpha]$ 不能作为复平面上的格表出. 例如，环 $\mathbb{Z}\left[\frac{1}{2}\right]$ 由可以表达为 $\frac{1}{2}$ 的整系数多项式的有理数组成. 这些有理数可以简单地描述为分母为 2 的幂的那些有理数. 它们构成实直线的一个稠密子集.

一个复数 α 称为*代数的*，如果它是一个整系数多项式的根，即如果某个形如(1.2)的表达式为零. 例如，$i+3$，$1/7$，$7+\sqrt[3]{2}$ 及 $\sqrt{3}+\sqrt{-5}$ 都是代数数.

如果不存在以 α 为根的整系数多项式，则称 α 为一个*超越数*. 数 e 和 π 是超越数，虽然不容易证明它们是超越数. 如果 α 是超越的，那么两个不同的形如(1.2)的多项式表达式必表示两个不同的复数. 在这种情形下，通过规则 $p(x)\leftrightarrow p(\alpha)$，环 $\mathbb{Z}[\alpha]$ 的元素与整系数多项式 $p(x)$ 一一对应.

当 α 为代数数时，存在许多代表同一个复数的多项式表达式(1.2). 例如当 $\alpha=i$ 时，幂 α^n 取四个值 ±1，$\pm i$. 利用关系 $i^2=-1$，每个表达式(1.2)可化为 i 的次数 $\leqslant 1$ 的表达式. 这与上面给出的高斯整数环的描述是一致的.

代数数和超越数这两类数，在某种程度上类似于循环群的两种可能：有限的和无限的[第二章(2.7)].

抽象环的定义除了不要求存在乘法的逆外，与域的定义是类似的[第三章(2.3)].

【1.3】定义 环 R 是一个具有称为加法和乘法的两个合成法则 $+$ 和 $\times$ 的集合，其合成法则满足下列公理：

(a) R 关于合成法则 $+$ 是一个阿贝尔群，单位元记作 0. 这个阿贝尔群记作 R^+.

(b) 乘法是结合的，具有单位元，记作 1.

(c) 分配律：对所有 a，b，$c\in R$，

$$(a+b)c = ac+bc \quad 及 \quad c(a+b) = ca+cb.$$

环的子环是一个在加法、减法、乘法运算下封闭且包含 1 的子集.

所使用的术语并不完全是标准的. 有时在定义中并未要求环中有乘法单位元. 本书中主要学习交换环，即对于乘法满足交换律 $ab=ba$ 的环. 这样除非明确提到非交换性，我们约定环这个词意为有单位元的交换环. 对于交换环两个分配律(c)是等价的.

所有实元素的 $n\times n$ 矩阵的环 $\mathbb{R}^{n\times n}$ 是非交换环的一个重要例子. 346

除了 $\mathbb{C}$ 的子环，最重要的环是多项式环. 给定任意环 R，系数在 R 中的 x 的多项式是一个形如

【1.4】
$$a_nx^n+\cdots+a_1x+a_0$$

的表达式，其中 $a_i\in R$. 这些多项式的集合构成一个环，通常记为 $R[x]$. 我们将在下一节讨论多项式环.

下面是另外一些环的例子：

【1.5】例

(a) 任意域是一个环.

(b) 实变量 x 的连续实值函数的集合 $\mathcal{R}$ 构成一个环，函数的加法与乘法为：

$$[f+g](x)=f(x)+g(x) \quad 及 \quad [fg](x)=f(x)g(x).$$

(c) 由单独一个元素 0 构成的零环 $R=\{0\}$.

在域的定义[第三章(2.3)]中，要求乘法单位元 1 属于 $F^\times=F-\{0\}$. 因此一个域至少有两个不同的元素，即 0 和 1. 在环中并未排除关系 $1=0$，但这仅会发生一次：

【1.6】命题 设 R 是满足 $1=0$ 的环，则 R 是零环.

证明 首先注意到对环 R 中的任意元素 a 有 $0a=0$. 证明与向量空间的情形相同[第三章(1.6a)]. 假设在 R 中 $1=0$，并设 a 是 R 中的任意元素. 则有 $a=1a=0a=0$. 因而 R 的每个元素都是 0. 这说明 R 是零环. ∎

虽然在环中不要求乘法逆的存在，但某些特定的元素会有逆元，并且逆元一旦存在就是唯一的. 具有乘法逆的元素称为单位. 例如，整数环的单位为 1 和 -1，而实多项式的环 $\mathbb{R}[x]$ 的单位是非零常数多项式. 域是非零环并且其中每一个非零元都是单位.

环的单位元 1 总是 1 个单位，只要提到环 R 的单位元(“the” unit element)就是指单位元(identity). 这是个含混的术语，但要改变它已经太晚了.

第二节 整数和多项式的形式构造

我们学过环的公理对整数成立. 现在再看一看要写出像结合律和分配律这样的性质的证明需要什么. 完整的证明需要写很多，我们在这里只开个头. 习惯上从定义正整数的加法和乘法 347

开始．负数在后面才会引入．这意味着在证明的过程中要处理种种情形，这是令人厌烦的，不然就要找到一个聪明的记号来避免这种按情形的分析．我们将满足于对正整数上运算的描述．正整数也称作*自然数*．

自然数集N由称为*佩亚诺公理*的下面的这些性质刻画：

【2.1】

(a) 集合N含有一个特别的元素 1．

(b) *后继函数*：存在一个映射 σ：N ⟶N将每个整数 $n\in$ N映到另一个整数，称之为*下一个整数*或*后继*．这是个单射，且对每个 $n\in$ N，$\sigma(n)\neq 1$．

(c) *归纳公理*：假设N的子集有这些性质：

(i) $1\in S$；

(ii) 如果 $n\in S$ 则 $\sigma(n)\in S$．

则 S 包含每一个自然数：$S=$ N．

当加法定义以后，下一个整数 $\sigma(n)$ 变成 $n+1$．但在现在记号 $n+1$ 会引起混乱．最好是用一个中性的记号，我们常将后继记为 $n'[=\sigma(n)]$．注意假设 σ 是单射，因而如果 m，n 是不同的整数，即如果 $m\neq n$，则 m'，n' 也是不同的整数．

后继函数使得能够使用自然数计数，这是算术的基础．

性质(c)是整数的归纳性质．直观上说自然数是从 1 开始通过不断地取下一个整数得到的：N $=\{1, 1', 1'', \cdots\}(=\{1, 2, 3, \cdots\})$，即数遍所有自然数．这个性质是归纳证明的正式基础．

假设要对每个正整数 n 证明一个论断 P_n，并令 S 是使 P 成立的整数集合．说 P_n 对每个整数成立与说 $S=$ N是一回事．对这个集合 S，归纳公理翻译成通常的归纳步骤：

【2.2】

(i) P_1 成立；

(ii) 如果 P_n 成立，则 $P_{n'}$ 成立．

也可用佩亚诺公理作递归定义．术语*递归定义*或*归纳定义*是指由自然数做指标的一系列对象 C_n 的定义，其中每一个对象是用其前一个来定义的．函数 $C_n=x^n$ 就是一个这样的例子．这个函数的一个递归定义是

348

$$x^1 = x \quad 而 \quad x^{n'} = x^n x.$$

其要点如下：

【2.3】

(i) 定义 C_1；

(ii) 给出一个由 C_n 确定 $C_n'(=C_{n+1})$ 的法则．

直观上看显然(2.3)唯一地确定序列 C_n，但要用佩亚诺公理来证明它就得有技巧．一个自然的证明方法如下：设 S 是使得对每个 $k\leqslant n$，(2.3)确定 C_k 的整数 n 的集合．于是(2.3i)表明 $1\in S$．而且(2.3ii)表明如果 $n\in S$，则 $n'\in S$．递归公理表明 $S=$ N，因此对每个 n，C_n 是唯一定义的．不幸的是关系$\leqslant$不包含在佩亚诺公理中，因此在开始之前要先定义它并推导其性质．

因而基于这个方法的证明会很长，我们将不在这里进行证明.

给定正整数集合并可以作递归定义后，我们可以如下定义正整数的加法和乘法：

【2.4】 加法：$m+1=m'$， $m+n'=(m+n)'$.

乘法：$m\cdot 1=m$， $m\cdot n'=m\cdot n+m$.

在这些定义中，我们取一个任意的整数 m 然后对这个整数 m 和每一个 n 递归地定义加法和乘法. 这样，对所有的 m，n 都定义了 $m+n$ 和 $m\cdot n$.

对整数的结合律、交换律和分配律的证明都是归纳法的练习，可以称作"佩亚诺游戏". 这里作为范例我们证明其中的两个.

加法结合律的证明 我们要证明对于所有 a，b，$n\in\mathrm{N}$，$(a+b)+n=a+(b+n)$. 首先对所有 a，b，验证 $n=1$ 的情形. 应用定义(2.4)三次得到

$$(a+b)+1=(a+b)'=a+b'=a+(b+1).$$

其次，假设结合律对所有 a，b 和特定的 n 值成立. 然后对 n' 作如下验证：

$$\begin{aligned}(a+b)+n' &= (a+b)+(n+1) \quad (\text{定义})\\ &= ((a+b)+n)+1 \quad (n=1\ \text{的情形})\\ &= (a+(b+n))+1 \quad (\text{归纳假设})\\ &= a+((b+n)+1) \quad (n=1\ \text{的情形})\\ &= a+(b+(n+1)) \quad (n=1\ \text{的情形})\\ &= a+(b+n') \quad (\text{定义}).\end{aligned}$$

■

乘法交换律的证明(假定加法交换律已得证) 我们先证明下面的引理：

【2.5】

$$m'\cdot n=m\cdot n+n.$$

349

$n=1$ 的情形是显然成立的：$m'\cdot 1=m'=m+1=m\cdot 1+1$. 因而假设对特定的 n 和对所有 m 的值(2.5)成立. 我们对 n' 进行验证：

$$\begin{aligned}m'\cdot n' = m'\cdot n+m' &= m'\cdot n+(m+1) \quad (\text{定义})\\ &= (m\cdot n+n)+(m+1) \quad (\text{归纳})\\ &= (m\cdot n+m)+(n+1) \quad (\text{加法的各种运算律})\\ &= m\cdot n'+n' \quad (\text{定义}).\end{aligned}$$

■

其次，对 n 归纳证明 $1\cdot n=n$. 最后，在已知 $m\cdot 1=m=1\cdot m$ 时，对 n 归纳证明 $m\cdot n=n\cdot m$：设它对 n 成立. 于是 $m\cdot n'=m\cdot n+m=n\cdot m+m=n'\cdot m$，这正是要证的.

加法和乘法其他性质的证明由类似的方法得到.

我们现在转到多项式环的定义. 可以定义系数属于任意环 R 的多项式的概念，这是指变量的幂的线性组合：

【2.6】

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

其中 $a_i\in R$. 这样的表达式常称为*形式多项式*，以将它们区别于多项式函数. 每个实系数形式多项式确定一个实数上的多项式函数.

(2.6)中出现的变量 x 是一个任意符号，单项式 x^i 视为无关的. 这是指如果

$$g(x)=b_m x^m+b_{m-1}x^{m-1}+\cdots+b_1 x+b_0$$

是另一个系数在 R 中的多项式，则 $f(x)$ 与 $g(x)$ 相等当且仅当对所有 $i=0$，1，2，…，有 $a_i=b_i$.

非零多项式的次数是使得 x^k 的系数 a_k 不为零的最大整数 k.（零多项式的次数被认为是不确定的.）非零多项式的最高次系数称为*首项系数*，首项系数为 1 的多项式称为*首一多项式*.

多项式的某些系数可能为零从而造成麻烦．我们得去掉系数为零的项：例如 $x^2+3=0x^3+x^2+3$．这样多项式 $f(x)$ 有不止一个表示(2.6)．标准化记号的方法之一是只列出非零系数，即在(2.6)中略去所有 $0x^i$ 的项．但在计算过程中可能产生零系数，得把它们抛弃．另一种可能是坚持(2.6)中最高次数项系数 a_n 非零并列出所有低次项．同样的问题也会出现．因而在描述环的结构时，对这样的约定需要讨论一些特殊的情形．这是令人恼火的，因为由零系数导致的歧义并不是件有趣的事.

围绕记号问题的一个办法是不管是否为 0，列出所有单项式的系数．这对计算并不有利，

350 但却能有效地验证环的公理．因此为了定义环的运算，我们将把多项式写为标准形式

【2.7】
$$f(x)=a_0+a_1x+a_2x^2+\cdots,$$

其中系数 a_i 都属于环 R 并且仅有*有限多个系数不为零*．形式上，多项式(2.7)由其系数 a_i 的向量(或序列)

【2.8】
$$a=(a_0,a_1,\cdots)$$

确定，其中 $a_i\in R$ 且除了有限多个 a_i 外全都为零．每个这样的向量对应于一个多项式．在 R 是域的情形，这些无穷向量构成具有在第三章(5.2d)中定义的无穷基 e_i 的向量空间 Z．向量 e_i 对应于*单项式* x^i，且单项式构成所有多项式空间的一个基.

多项式的加法和乘法仿照熟知的实多项式函数的运算进行．设 $f(x)$ 如上，并设

【2.9】
$$g(x)=b_0+b_1x+b_2x^2+\cdots$$

是由向量 $b=(b_0，b_1，\cdots)$ 所确定的另一个系数属于同一个环 R 的多项式．f 与 g 的和是

【2.10】
$$f(x)+g(x)=(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots$$
$$=\sum_k(a_k+b_k)x^k,$$

它对应于向量加法：$a+b=(a_0+b_0，a_1+b_1，\cdots)$.

两个多项式 f，g 的乘积通过逐项相乘并且合并 x 的相同次数的系数进行计算．如果用分配律展开乘积而不合并项，我们得到

【2.11】
$$f(x)g(x)=\sum_{i,j}a_ib_jx^{i+j}.$$

注意只有有限多个非零系数 a_ib_j．这是个正确的公式，但右边并不是标准形式(2.7)，这是因为同一单项式 x^n 出现多次——每一对使 $i+j=n$ 的指标 i，j 都会出现一次．因而需要把项合并起来而使右边变成标准形式．这引出定义

$$f(x)g(x)=p_0+p_1x+p_2x^2+\cdots,$$

其中

【2.12】
$$p_k=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0=\sum_{i+j=k}a_ib_j.$$

351 然而，在进行计算时会希望晚些时候再合并项.

【2.13】**命题** 在多项式集合 $R[x]$ 上存在唯一的具有下列性质的交换环结构：

(a) 多项式的加法是向量加法(2.10).

(b) 单项式的乘法由规则(2.12)给出.

(c) 当将 R 的元素与常值多项式等同时，环 R 是 $R[x]$ 的子环.

这个命题的证明在记号上令人不快而且没有什么令人感兴趣的特性. 因而我们将其省去.

多项式对环的理论是基本的，并且我们还必须考虑像 $x^2y^2+4x^3-3x^2y-4y^2+2$ 这样的多变量的多项式. 在定义上并没有太大的变化.

设 x_1，…，x_n 为变量. 单项式是这些变量的一个形如

$$x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$$

的乘积，其中指数 i_ν 是非负整数. 指数的 n-元组(i_1，…，i_n)确定单项式. 这样一个 n-元组称为一个多重指标，多重指标的向量记号 $i=(i_1, \cdots, i_n)$ 是非常方便的. 利用它可将单项式写为

【2.14】
$$x^i = x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}.$$

单项式 x^0 记为 1，其中 $0=(0, \cdots, 0)$.

一个系数属于环 R 的多项式是一个系数属于 R 的有限多个单项式的线性组合. 使用简写记号(2.14)，任意多项式 $f(x)=f(x_1, \cdots, x_n)$ 可以恰好以一种方式写为

【2.15】
$$f(x) = \sum_i a_i x^i$$

的形式，其中 i 取遍所有多重指标(i_1，…，i_n)，系数 a_i 属于 R 并且这些系数中仅有有限多个是非零的.

由一个 R 的非零元素乘上一个单项式的积得到的多项式也称为单项式. 这样如果 $r\in R$ 非零且如果 x^i 如上(2.14)，则

【2.16】
$$m = rx^i$$

是一个单项式. 单项式可以看作是恰有一个非零系数的多项式.

使用多重指标记号，公式(2.10)和(2.12)定义了多变量多项式的加法和乘法，且命题(2.13)类似的结果成立.

系数在 R 中的多项式环用下面两个符号之一表示：

【2.17】
$$R[x_1,\cdots,x_n] \quad 或 \quad R[x],$$

352

其中符号 x 理解为变量的集合(x_1，…，x_n). 在没有引入变量集合时，$R[x]$ 是指一个变量 x 的多项式环.

第三节 同态与理想

从一个环到另一个环的同态 $\varphi: R \longrightarrow R'$ 是一个与合成法则相容并且将 1 变到 1 的映射，即一个对所有 a，$b\in R$ 满足

【3.1】
$$\varphi(a+b) = \varphi(a)+\varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(1_R) = 1_{R'}$$

的映射. 环的同构是一个双射的同态. 如果存在一个同构 $R \longrightarrow R'$，两个环称为是同构的.

有必要对(3.1)的第三部分说几句话. 同态 φ 与加法相容蕴涵它是群的一个同态 $R^+ \longrightarrow$

R'^+. 我们知道一个群同态把单位元变到单位元，从而 $\varphi(0)=0$. 但 R 关于×不是群，我们不能由与乘法的相容性得到 $\varphi(1)=1$. 因而条件 $\varphi(1)=1$ 必须单独列出. 例如，将 R 的所有元素映到零的零映射 $R^+ \longrightarrow R'^+$ 与+和×相容，但除非在 R' 中 $1=0$，否则它不能将 1 映到 1. 也就是说除非 R' 是零环，否则零映射不是环同态[见(1.6)].

最重要的环同态是那些通过对多项式取值所得到的同态. 实多项式在一个实数 a 的取值定义了一个同态

【3.2】 $$\mathbb{R}[x] \longrightarrow \mathbb{R}, \quad 使得\ p(x) \rightsquigarrow p(a).$$

我们也可以让实多项式在一个如 i 这样的复数取值而得到一个同态

【3.3】 $$\mathbb{R}[x] \longrightarrow \mathbb{C}, \quad 使得\ p(x) \rightsquigarrow p(\mathrm{i}).$$

多项式取值原理的一般性陈述是：

【3.4】命题 代入原理：设 $\varphi: R \longrightarrow R'$ 是一个环同态.

(a) 给定一个元素 $\alpha \in R'$，存在唯一的同态 Φ: $R[x] \longrightarrow R'$，它在常多项式上与映射 φ 一致并使得 $x \rightsquigarrow \alpha$.

(b) 更一般地，给定元素 $\alpha_1, \cdots, \alpha_n \in R'$，存在唯一的从 n 个变量的多项式环到 R' 的同态 Φ: $R[x_1, \cdots, x_n] \longrightarrow R'$，它在常多项式上与映射 φ 一致并使得对 $\nu=1, \cdots, n$ 有 $x_\nu \rightsquigarrow \alpha_\nu$.

证明 用指标的向量记号，(b)的证明与(a)的相同. 我们将一个元素 $r \in R$ 在 R' 中的象记作 r'. 使用 Φ 是在 R 上限制为 φ 并且将 x_ν 映到 α_ν 的同态这个事实，我们发现它通过

353

【3.5】 $$\sum r_i x^i \rightsquigarrow \sum \varphi(r_i)\alpha^i = \sum r'_i \alpha^i$$

在多项式 $f(x)=\sum r_i x^i$ 上作用. 换言之，Φ 在多项式的系数上作用为 φ，并且它用 α 代替 x. 因为这个公式为我们描述了 Φ，这证明了代入同态的唯一性. 为证明它的存在性，我们将公式取为 Φ 的定义，并证明这个映射是一个同态 $R[x] \longrightarrow R'$. 容易证明 Φ 将 1 映到 1 并且它与多项式的加法相容. 用(2.11)可以验证与乘法的相容性：

$$\Phi(fg)=\Phi(\sum a_i b_j x^{i+j})=\sum \Phi(a_i b_j x^{i+j})=\sum_{i,j} a'_i b'_j \alpha^{i+j}$$
$$=(\sum_i a'_i \alpha^i)(\sum_j b'_j \alpha^j)=\Phi(f)\Phi(g).$$ ■

下面是系数环 R 改变时代入原理的例子：设 ψ: $R \longrightarrow R_1$ 是一个环同态. 将 ψ 与作为 $R_1[x]$ 的子环的 R_1 的包含合成，得到一个同态 $\varphi: R \longrightarrow R_1[x]$. 代入原理断言存在唯一一个 φ 扩张为同态 Φ: $R[x] \longrightarrow R_1[x]$ 使得 $x \rightsquigarrow x$. 这是一个在多项式的系数上作用并使变量 x 不变的映射. 如果用 a' 表示 $\psi(a)$，则它将多项式 $a_n x^n + \cdots + a_1 x + a_0$ 映到 $a'_n x^n + \cdots + a'_1 x + a'_0$.

一个重要的情形是同态 $\mathbb{Z} \longrightarrow \mathbb{F}_p$，其中 $F_p = \mathbb{Z}/p\mathbb{Z}$ 为 p 元域. 这个映射扩张成为一个同态

【3.6】 $$\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x], 使得$$
$$f(x) = a_n x^n + \cdots + a_0 \rightsquigarrow \bar{a}_n x^n + \cdots + \bar{a}_0 = \bar{f}(x),$$

其中 $\bar{a}_i$ 表示 a_i 模 p 的剩余类. 自然也将多项式 $\bar{f}(x)$ 称为 $f(x)$ 模 p 的剩余.

代入原理也是证明多项式环的各种构造等价的一个有效方法；同构

$$R[x,y] \approx R[x][y]$$

是一个典型的例子．这里右边表示以 x 的多项式为系数的变量 y 的多项式的环．这两个环同构这一断言是一个多项式 $f(x, y)$ 可以按 y 的相同次数合并项而将它写为 y 的多项式这一事实的一个正式的阐述．例如，

$$x^2y^2+4x^3-3x^2y-4y^2+2$$
$$=(x^2-4)y^2-(3x^2)y+(4x^3+2).$$

【3.7】推论　设 $x=(x_1, \cdots, x_m)$ 及 $y=(y_1, \cdots, y_n)$ 表示变量的集合．存在唯一的同构 $R[x, y]\longrightarrow R[x][y]$，它在 R 上是恒等映射并将变量映为它们自己．

354

证明　注意 R 是 $R[x]$ 的子环而 $R[x]$ 是 $R[x][y]$ 的子环．因而 R 是 $R[x][y]$ 的子环．考虑包含映射 $\varphi: R\longrightarrow R[x][y]$．代入原理(3.4)告诉我们存在唯一的同态 Φ：$R[x, y]\longrightarrow R[x][y]$ 拓广这一映射并将变量 x_μ，y_ν 映到我们想要的地方．因而可将变量映到它们自身．这样构造的映射 Φ 就是所需的同构．可以再次用代入原理证明它有一个逆：我们注意到 $R[x]$ 是 $R[x, y]$ 的子环，因而可将包含映射 ψ：$R[x]\longrightarrow R[x, y]$ 通过将 y_j 映到自身而扩张为一个映射 Ψ：$R[x][y]\longrightarrow R[x, y]$．合成同态 $\Psi\Phi$：$R[x, y]\longrightarrow R[x, y]$ 在 R 及 $\{x_\mu, y_\nu\}$ 上都是恒等映射．由代入同态的唯一性，$\Psi\Phi$ 是恒等映射．同样地，$\Phi\Psi$ 也是恒等映射．这就证明了 Φ 是同构．■

由于实多项式 $f(x)$ 可在实数上取值，因此它在实直线上定义一个多项式函数．术语多项式常指这样得到的函数，这样做没什么危险，因为我们可以由多项式的函数重新得到多项式：

【3.8】命题　设 $\mathcal{R}$ 表示 $\mathbb{R}^n$ 上的实值连续函数的环．则将多项式映到其相伴的多项式函数的映射 $\varphi: \mathbb{R}[x_1, \cdots, x_n]\longrightarrow\mathcal{R}$ 是一个单同态．

证明　这个同态的存在性由代入原理得到．我们证明其单射性．只需要证明如果与多项式 $f(x)$ 相伴的函数是零函数，则 $f(x)$ 是零多项式．设相伴的多项式函数是 $\tilde{f}(x)$．如果 $\tilde{f}(x)$ 恒等于零，则其所有导数也都为零．另一方面，可以用微分多项式函数的规则求形式多项式的微分．如果多项式 f 的某个系数非零，则适当阶导数的常数项也将非零．从而这个导数在原点非零，因而 $\tilde{f}(x)$ 不是零函数．■

环同态的另一个重要例子是从整数到任意环的映射：

【3.9】命题　从整数环到任意环 R 恰有一个同态

$$\varphi: \mathbb{Z}\longrightarrow R.$$

它是如下定义的映射：如果 $n>0$，则 $\varphi(n)=$"n 乘以 1_R"$=1_R+\cdots+1_R$（n 次），并且 $\varphi(-n)=-\varphi(n)$．

证明概述　设 $\varphi: \mathbb{Z}\longrightarrow R$ 是一个同态．由同态的定义，$\varphi(1)=1_R$，且 $\varphi(n+1)=\varphi(n)+\varphi(1)$．故 φ 在自然数上由递归定义

$$\varphi(1)=1 \quad 和 \quad \varphi(n')=\varphi(n)+1$$

355

确定，其中′表示后继函数(2.1b)．这个公式连同 $n>0$ 时 $\varphi(-n)=-\varphi(n)$ 及 $\varphi(0)=0$，唯一确定 φ．故上面的映射是仅有的可能的映射．要给出这个映射是同态的一个正式证明，又得回到佩亚诺公理．我们验证 φ 与正整数的加法相容．要证 $\varphi(m+n)=\varphi(m)+\varphi(n)$，我们注意到由 φ 的定义，当 $n=1$ 时这是成立的．假设它对所有 m 及某个特定的 n 成立．则对所有 m 及 n' 证明它也成立：

$$
\begin{aligned}
\varphi(m+n') &= \varphi((m+n)+1) \quad (\text{整数加法的性质}) \\
&= \varphi(m+n)+1 \quad (\varphi\text{ 的定义}) \\
&= \varphi(m)+\varphi(n)+1 \quad (\text{归纳假设}) \\
&= \varphi(m)+\varphi(n') \quad (\varphi\text{ 的定义}).
\end{aligned}
$$

由归纳法，对所有的 m 和 n，$\varphi(m+n)=\varphi(m)+\varphi(n)$. 我们将其与正整数乘法的相容性留作练习. ■

这个映射使得能够确定整数在任意环 R 中的象. 这样可以将 R 中的符号 3 解释为元素 $1+1+1$，并且可以将诸如 $3x^2+2x$ 这样的整多项式解释为多项式环 $R[x]$ 中的一个元素.

现在回到任意的环同态 $\varphi:R\longrightarrow R'$. 用与群同态的核同样的方式定义 φ 的核：

$$\ker\varphi=\{a\in R\mid \varphi(a)=0\}.$$

回顾群同态的核是子群，而且它是正规的[第二章(4.9)]. 同样地，环同态的核在环的加法和乘法运算之下是封闭的，而且它还有比在乘法下封闭更强的性质：

【3.10】 如果 $a\in\ker\varphi$ 且 $r\in R$，则 $ra\in\ker\varphi$.

因为如果 $\varphi(a)=0$，则 $\varphi(ra)=\varphi(r)\varphi(a)=\varphi(r)0=0$. 另一方面，除非它是整个环 R，否则 $\ker\varphi$ 不包含 R 的单位元 1，因而核不是子环.（如果 $1\in\ker\varphi$，则对所有 $r\in R$，有 $r=r1\in\ker\varphi$.）而且如果 $\ker\varphi=R$，则 φ 是零映射，如上面所述，R' 是零环.

例如，设 φ 是由在实数 2 上的取值定义的同态 $\mathbb{R}[x]\longrightarrow\mathbb{R}$. 则 $\ker\varphi$ 是以 2 为根的多项式集合. 它亦可描述为能被 $x-2$ 整除的多项式的集合.

环同态的核的性质——它在由环的任意一个元素相乘之下封闭——抽象为理想的概念. 由定义，环 R 的一个理想 I 是 R 的具有下列性质的子集：

【3.11】

(i) I 是 R^+ 的子群；

356

(ii) 如果 $a\in I$ 而 $r\in R$，则 $ra\in I$.

这个特别的术语"理想"是以前在数论中所使用的"理想元素"的简称. 我们将在第十一章看到这个术语是如何引出的. 性质(ii)蕴涵了理想在乘法下封闭，但它更强. 将性质(i)和(ii)一齐考虑的一个好办法是下面这个等价的叙述：

【3.12】 I 非空，且以 $r_i\in R$ 为系数的元素 $a_i\in I$ 的线性组合 $r_1a_1+\cdots+r_ka_k$ 属于 I.

在任意环 R 中，一个特定元素 a 的倍数(或等价地，能被 a 整除的元素)的集合构成一个理想，称为由 a 生成的主理想. 这个理想将由下列方式之一表示：

【3.13】 $$(a)=aR=Ra=\{ra\mid r\in R\}.$$

这样通过在 2 取值定义的同态 $\mathbb{R}[x]\longrightarrow\mathbb{R}$ 的核可以表示为 $(x-2)$ 或 $(x-2)\mathbb{R}[x]$. 实际上主理想的记号 (a) 虽然方便，但由于没提到环，所以不是太清楚. 例如，$(x-2)$ 根据其所处的上下文，可以表示 $\mathbb{R}[x]$ 中的理想，也可以表示 $\mathbb{Z}[x]$ 中的理想. 当有几个环时，最好使用其他记号.

也可以考虑由 R 中元素 $a_1,\cdots,a_n$ 的集合生成的理想 I，它定义为包含这些元素的最小的理想. 它可以描述为系数 r_i 在环中的所有线性组合

【3.14】 $$r_1a_1+\cdots+r_na_n$$

的集合. 因为如果理想包含 a_1, …, a_n, 则(3.12)告诉我们它也包含这些元素的每一个线性组合. 另一方面，线性组合的集合在加法、减法及用 R 中元素作的乘法下是封闭的. 因而它是理想 I. 这个理想通常记作

【3.15】 $$(a_1,\cdots,a_n)=\{r_1a_1+\cdots+r_na_n \mid r_i\in R\}.$$

例如，如果 R 是整多项式环 $\mathbb{Z}[x]$，则记号 $(2, x)$ 表示 2 和 x 的具有整多项式系数的线性组合的理想. 这个理想也可表述为所有常数项能被 2 整除的整多项式 $f(x)$ 的集合. 它是由 $f(x)\rightsquigarrow(f(0)$ 的剩余(模 2))定义的同态 $\mathbb{Z}[x]\longrightarrow\mathbb{Z}/2\mathbb{Z}$ 的核.

本节的其余部分将描述一些简单情形的理想. 在任意环中，由单独一个零组成的集合是一个理想，称之为*零理想*. 它显然是一个主理想，整个环也是. 作为由元素 1 生成的理想，R 称为*单位理想*，通常记作(1). 单位理想是包含单位的仅有的理想. 不是(0)或(1)的理想称为*真理想*.

域可以由它们没有真理想这一事实来刻画.

【3.16】命题

(a) 设 F 是域. 则 F 仅有的理想是零理想和单位理想.

(b) 反之，如果一个环 R 恰好只有两个理想，则 R 是一个域.

我们来证明(b). 假设 R 恰好有两个理想. 使域区别于环的性质是 $1\neq 0$ 及每个非零元素 $a\in R$ 有一个乘法逆. 如前所见，$1=0$ 只会在有一个元素的零环中才出现. 而这个环只有一个理想. 因为我们的环有两个理想，所以在 R 中 $1\neq 0$. 两个理想(1)和(0)是不同的，因而它们是 R 仅有的两个理想.

现在证明 R 的每一个非零元素有一个逆. 设 $a\in R$ 是一个非零元，考虑主理想 (a). 因为 $a\in(a)$,所以 $(a)\neq(0)$. 因而 $(a)=(1)$. 这说明 1 是 a 的一个倍数，比如 ra. 等式 $ar=1$ 表明 a 有一个逆.

【3.17】推论 *设 F 是域而 R' 是非零环. 每个同态 $\varphi:F\longrightarrow R'$ 是单射.*

证明 我们应用(3.16). 如果 $\ker\varphi=(1)$，则 φ 为零映射. 但由于 R' 不是零环，因此零映射不是同态. 因而 $\ker\varphi=(0)$. ■

容易确定整数环的理想.

【3.18】命题 *整数环 $\mathbb{Z}$ 的每个理想都是主理想.*

这是因为整数加法群 $\mathbb{Z}^+$ 的每个子群具有 $n\mathbb{Z}$ 的形式[第二章(2.3)]，而这些子群恰好是主理想.

环 R 的特征是生成同态 $\varphi:\mathbb{Z}\longrightarrow R(3.9)$ 的核的非负整数 n. 这意味着 n 是使得“n 乘上 1_R”$=0$ 的最小正整数，或者，如果核为(0)，则特征为零(见第三章第二节). 这样 $\mathbb{R}$，$\mathbb{C}$ 和 $\mathbb{Z}$ 的特征为零，而 p 元素域 $\mathbb{F}_p$ 的特征为 p.

整数环的每个理想是主理想的证明可作适当改动而用来证明多项式环 $F[x]$ 的每个理想是主理想. 为此，我们需要多项式的带余除法.

【3.19】命题 *设 R 是环并设 f，g 是 $R[x]$ 的多项式. 假设 f 的首项系数是 R 的一个单位. (例如，当 f 是首一多项式时这是成立的.)则存在多项式 q，$r\in R[x]$ 使得*

357

$$g(x) = f(x)q(x) + r(x),$$

且余式 r 的次数小于 f 的次数或者 $r=0$.

带余除法可以通过对 g 的次数作归纳加以证明.

注意当系数环为域时，只要存在首项系数，即 $f\neq 0$，就满足 f 的首项系数为单位的这个假设.

【3.20】推论 设 $g(x)$ 是 $R[x]$ 中的首一多项式，并设 α 是使得 $g(\alpha)=0$ 的 R 的元素. 则 $x-\alpha$ 在 $R[x]$ 中整除 g.

358

【3.21】命题 设 F 是域. 单个变量 x 的多项式环 $F[x]$ 的每个理想都是主理想.

证明 设 I 是 $F[x]$ 的理想. 由于零理想是主理想，可以假设 $I\neq(0)$. 求 $\mathbb{Z}$ 的非零子群的生成元的第一步是选择其中最小的正整数. 这里改为选择具有极小次数的非零多项式 f. 我们断言 I 是由 f 生成的主理想. 由理想的定义可知主理想 (f) 包含在 I 中. 要证 $I\subset(f)$，我们用带余除法记 $g=fq+r$，其中除非 r 为零，否则它的次数小于 f 的次数. 现在如果 g 属于理想 I，则由于 $f\in I$，理想的定义表明 $r=g-fq$ 亦属于 I. 由于 f 在非零元素中有极小次数，仅有的可能性是 $r=0$. 这样 f 整除 g，这正是要证的. ∎

下面的推论的证明与第二章中(2.6)的证明是类似的.

【3.22】推论 设 F 是域，并设 f，g 是 $F[x]$ 中不全为零的多项式. 存在唯一的首一多项式 $d(x)$，称为 f 和 g 的最大公因式，具有下列性质：

(a) d 生成 $F[x]$ 中由两个多项式 f，g 生成的理想 (f, g).

(b) d 整除 f 和 g.

(c) 如果 h 是 f 和 g 的因子，则 h 整除 d.

(d) 存在多项式 p，$q\in F[x]$ 使得 $d=pf+qg$.

第四节 商环与环的关系

设 I 是环 R 的理想. R^+ 的加法子群 I^+ 的陪集是子集

$$a+I,\quad a\in R.$$

由对群所作的证明得到陪集的集合 $R/I=\overline{R}$ 在加法下是一个群. 它也是一个环：

【4.1】定理 设 I 是环 R 的理想.

(a) 陪集的集合 $\overline{R}=R/I$ 上存在唯一的环结构，使得使 $a \rightsquigarrow \overline{a}=a+I$ 的典范映射 π：$R\longrightarrow \overline{R}$ 是一个同态.

(b) π 的核为 I.

证明 这个证明在 R 是整数环的特殊情形中已经用过(第二章第九节). 我们想在 $\overline{R}$ 上加上具有所需性质的环的结构，而且如果忘掉乘法而只考虑加法法则的话，证明已经给出了[第二章(10.5)]. 剩下要做的是定义乘法. 设 x，$y\in\overline{R}$，比如 $x=\overline{a}=a+I$ 而 $y=\overline{b}=b+I$. 我们想要把乘积定义为 $xy=\overline{ab}=ab+I$. 与群的陪集乘法[第二章(10.1)]不同，积的集合

359

$$P=\{rs \mid r\in a+I, s\in b+I\}$$

并不总是 I 的陪集. 然而和整数环的情形一样，集合 P 总是包含在一个单独的陪集 $ab+I$ 中：

如果记 $r=a+u$ 和 $s=b+v$ 且 $u, v\in I$，则

$$(a+u)(b+v)=ab+(av+bu+uv),$$

由于 I 是理想，$av+bu+uv\in I$. 这是定义积陪集所需的一切：它是包含集合 P 的陪集. 由于陪集是 R 的划分，这个陪集是唯一的. 断言剩下的证明严格按照第二章第九节的方式进行. ■

如第六章(8.4)和第二章(10.9)一样，可以证明下面的命题：

【4.2】命题　商环的映射性质：

设 $f: R\longrightarrow R'$ 是一个核为 I 的环同态并设 J 是含于 I 的一个理想. 记剩余环 R/J 为 $\overline{R}$.

(a) 存在唯一同态 $\overline{f}: \overline{R}\longrightarrow R'$ 使得 $\overline{f}\pi=f$：

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ & \searrow^{\pi} \quad \nearrow_{\overline{f}} & \\ & \overline{R}=R/J & \end{array}.$$

(b) 第一同构定理：如果 $J=I$，则 $\overline{f}$ 将 $\overline{R}$ 同构地映到 f 的象上.

我们现在描述商环 R/J 的理想与原来的环 R 的理想之间的基本关系.

【4.3】命题　对应定理：设 $\overline{R}=R/J$，并设 π 表示典范映射 $R\longrightarrow\overline{R}$.

(a) 存在一个包含 J 的 R 的理想的集合与 $\overline{R}$ 的所有理想的集合之间的一一对应，如下给出：

$$I \rightsquigarrow \pi(I),\quad \pi^{-1}(\overline{I}) \leftsquigarrow \overline{I}.$$

(b) 如果 $I\subset R$ 对应于 $\overline{I}\subset\overline{R}$，则 R/I 与 $\overline{R}/\overline{I}$ 是同构的环.

命题的第二部分常被称为第三同构定理[还有第二同构定理(见第六章杂题练习 7)].

360

证明　要证(a)，必须验证以下几点：

(i) 如果 I 是 R 中包含 J 的理想，则 $\pi(I)$ 是 $\overline{R}$ 的理想.

(ii) 如果 $\overline{I}$ 是 $\overline{R}$ 的理想，则 $\pi^{-1}(\overline{I})$ 是 R 的理想.

(iii) $\pi^{-1}(\pi(\overline{I}))=I$ 及 $\pi(\pi^{-1}(\overline{I}))=\overline{I}$.

我们知道子群的象是子群[第二章(4.4)]. 因而要证 $\pi(I)$ 是 $\overline{R}$ 的理想，只需证明它在 $\overline{R}$ 的元素的乘积下封闭. 设 $\overline{r}\in\overline{R}$，并设 $\overline{x}\in\pi(I)$. 对 $r\in R$ 记 $\overline{r}=\pi(r)$，对 $x\in I$ 记 $\overline{x}=\pi(x)$. 则有 $\overline{rx}=\pi(rx)$ 且 $rx\in I$. 于是 $\overline{rx}\in\pi(I)$. 注意这个证明对 R 的所有理想都成立. 在此不必假设 $I\supset J$. 然而，π 是满射这一事实是很本质的.

其次，用 φ 表示同态 $\overline{R}\longrightarrow\overline{R}/\overline{I}$，考虑合成映射 $R\xrightarrow{\pi}\overline{R}\xrightarrow{\varphi}\overline{R}/\overline{I}$. 由于 π 和 φ 都是满射，因此 $\varphi\circ\pi$ 也是. 而且 $\varphi\circ\pi$ 的核是使得 $\pi(r)\in\overline{I}=\ker\varphi$ 的元素 $r\in R$ 的集合. 由定义，这是 $\pi^{-1}(\overline{I})$. 因此，作为同态的核，$\pi^{-1}(\overline{I})$ 是 R 的一个理想. 这证明了(ii). 对同态 $\varphi\circ\pi$ 应用第一同构定理从而证明 $R/\pi^{-1}(\overline{I})$ 同构于 $\overline{R}/\overline{I}$. 这就证明了命题中的(b).

还要证明(iii)；记住 π^{-1} 通常不是一个映射. 包含关系 $\pi^{-1}(\pi(I))\supset I$ 及 $\pi(\pi^{-1}(\overline{I}))\subset\overline{I}$ 是集合的任意映射以及对于任意子集的一般性质. 此外，等式 $\pi(\pi^{-1}(\overline{I}))=\overline{I}$ 对集合的任意满射成立. 我们略去这些事实的验证. 最后一点，$\pi^{-1}(\pi(I))\subset I$ 求 $I\supset J$. 设 $x\in\pi^{-1}(\pi(I))$. 则 $\pi(x)\in\pi(I)$，于是存在元素 $y\in I$ 使得 $\pi(y)=\pi(x)$. 由于 π 是同态，$\pi(x-y)=0$ 且 $x-y\in$

$J=\ker\pi$. 由于 $y\in I$ 而 $J\subset I$，这蕴涵$x\in I$,这正是要证的. ■

商构造有一个用环 R 的元素间的关系表述的重要解释. 我们想象在 R 的一些元素上作一系列的$+$，$-$，$\times$运算得到一个新元素 a. 如果所得的元素 a 是零，我们说给定的元素通过等式

【4.4】
$$a=0$$
联系起来. 例如，环$\mathbb{Z}$的元素 2，3，6 通过方程 $2\times3-6$ 联系起来.

如果元素 a 不是零，我们要问是否可能以某种方式修改 R 而使(4.4)成立. 可将此过程视为加上一个新的关系，它将会使环坍缩. 例如，在环$\mathbb{Z}$中关系 $3\times4-5$ 不成立，因为 $3\times4-5=7$. 但可以在整数中加上关系 $7=0$. 这样做相当于模 7 计算.

在这里可以忘掉得到特定元素 a 的过程；设它是 R 的一个任意元素. 当修改 R 加上关系 $a=0$ 时，我们想要保持运算$+$和$\times$，因而必须接受这个关系的后果. 例如，$ra=0$ 及 $b+a=b$ 是在 $a=0$ 两边乘上和加上给定元素得到的结果. 连续作这些运算可得到下面的结果

361

【4.5】
$$b+ra=b.$$
如果想要取 $a=0$，则对所有 b，$r\in R$ 也必须令 $b+ra=b$. 定理(4.1)告诉我们这就够了：(4.4)没有其他的结果. 为此，如果固定一个元素 b 而让 r 变动，集合$\{b+ra\}$是陪集 $b+(a)$，其中$(a)=aR$ 是由 a 生成的主理想. 对所有 r 令 $b+ra=b$ 与使该陪集的元素都相等是同一回事. 这正好是我们从 R 转到商环$\overline{R}=R/(a)$时所发生的. $\overline{R}$ 的元素为陪集$\overline{b}=b+(a)$，且典范映射 π：$R\longrightarrow\overline{R}$ 把一个陪集中的所有元素 $b+ra$ 映到同一个元素$\overline{b}=\pi(b)$. 这样在 $\overline{R}$ 中发生的坍缩的数量正好. 并且$\overline{a}=0$，因为 a 是理想(a)的一个元素，而后者是 π 的核. 因而将 $\overline{R}=R/(a)$视为通过在 R 中引入关系 $a=0$ 而得到的环是有道理的.

如果元素 a 是由一系列环运算从其他一些元素得到，如在(4.4)中所假设的，则 π 是同态这个事实蕴涵同样的运算序列在 $\overline{R}$ 中得到 0. 这样如果对某些 u，v，$w\in R$ 有 $uv+w=a$，则关系

【4.6】
$$\overline{u}\,\overline{v}+\overline{w}=0$$
在 $\overline{R}$ 中成立. 因为，由于 π 是同态，$\overline{u}\,\overline{v}+\overline{w}=\overline{uv+w}=\overline{a}=0$.

这一构造的一个很好的例子是整数环$\mathbb{Z}$中的关系 $n=0$. 得到的环是$\mathbb{Z}/n\mathbb{Z}$.

更一般地，通过取由 a_1，…，a_n 生成的理想 I(3.15)，(它是线性组合的集合$\{r_1a_1+\cdots+r_na_n\mid r_i\in R\}$)我们可以引入任意多个关系 $a_1=\cdots=a_n=0$. 商环 $\overline{R}=R/I$ 应视为通过在 R 中引入 n 个关系 $a_1=0$，…，$a_n=0$ 而得到的环. 由于 $a_i\in I$，剩余$\overline{a_i}$为零. R 的两个元素 b，b'在 $\overline{R}$ 中有相同的象当且仅当 $b'-b\in I$，或者说存在 $r_i\in R$，使得 $b'=b+r_1a_1+\cdots+r_na_n$. 这样关系

【4.7】
$$b+r_1a_1+\cdots+r_na_n=b$$
是 $a_1=\cdots=a_n=0$ 的仅有的结果.

由第三同构定理(4.3b)，每次引入一个关系与同时引入所有关系得到的结果是同构的. 精确地说，设 a，b 为环 R 的两个元素，设 $\overline{R}=R/(a)$是消去 a 所得的结果. 在环 $\overline{R}$ 上引入关系 $\overline{b}=0$ 得到商环$\overline{R}/(\overline{b})$，这个环同构于同时消去 a，b 得到的商环 $R/(a, b)$，因为(a, b)与$(\overline{b})$是对应的理想[见(4.3)].

注意我们引入的关系越多，在映射 $R \longrightarrow \bar{R}$ 下发生的坍缩就越厉害. 如果关系加得不小心，最坏时会发生最终得到 $I=R$ 而 $\bar{R}=0$ 的情况. 当将 R 坍缩为零环时，所有关系 $a=0$ 都成立.

362

在大多数情况下引入关系的过程会得到新环. 这是这个过程为什么重要的原因. 但在一些简单情形中可用第一同构定理将得到的环与较为熟悉的环联系起来. 我们用两个例子来说明这一点.

设 $R=\mathbb{Z}[\mathrm{i}]$为高斯整数环，并设 $\bar{R}$ 是由引入关系 $1+3\mathrm{i}=0$ 得到的环. 于是 $\bar{R}=R/I$，其中 I 是由 $1+3\mathrm{i}$ 生成的主理想. 我们先用关系做些实验，寻找一些可以认出的结果. 用$-\mathrm{i}$乘$-1=3\mathrm{i}$的两边，得到 $\mathrm{i}=3$. 因而在 $\bar{R}$ 中 $\mathrm{i}=3$. 另一方面，在 R 中 $\mathrm{i}^2=-1$，因而在 $\bar{R}$ 中亦有 $\mathrm{i}^2=-1$. 从而在 $\bar{R}$ 中 $3^2=-1$，或 $10=0$. 由于在 $\bar{R}$ 中 $\mathrm{i}=3$ 且 $10=0$，有理由猜想 $\bar{R}$ 同构于 $\mathbb{Z}/(10)=\mathbb{Z}/10\mathbb{Z}$.

【4.8】命题 环$\mathbb{Z}[\mathrm{i}]/(1+3\mathrm{i})$与整数模 10 的环$\mathbb{Z}/10\mathbb{Z}$同构.

证明 做了这一猜想后，我们可以通过分析同态 $\varphi:\mathbb{Z}\longrightarrow\bar{R}$(3.9)来证明它. 由第一同构定理，$\mathrm{im}\varphi\approx\mathbb{Z}/(\ker\varphi)$. 如果能证明 φ 是满射及 $\ker\varphi=10\mathbb{Z}$，就可完成证明. $\bar{R}$ 的每个元素是高斯整数 $a+b\mathrm{i}$ 的剩余. 由于在 $\bar{R}$ 中 $\mathrm{i}=3$，$a+b\mathrm{i}$ 的剩余与整数 $a+3b$ 的剩余相同. 这表明 φ 是满射. 其次，设 n 是 $\ker\varphi$ 的一个元素. 利用 $\bar{R}=R/I$ 这一事实，我们看到 n 一定属于理想 I，即在高斯整数环中 n 被 $1+3\mathrm{i}$ 整除. 因而对某两个整数 a，b，可以记 $n=(a+b\mathrm{i})(1+3\mathrm{i})=(a-3b)+(3a+b)\mathrm{i}$. 由于 n 是整数，$3a+b=0$ 或 $b=-3a$. 这样 $n=a(1-3\mathrm{i})(1+3\mathrm{i})=10a$. 这表明 $\ker\varphi\subset 10\mathbb{Z}$. 另一方面，我们已看到 $10\in\ker\varphi$. 因而 $\ker\varphi=10\mathbb{Z}$，这正是要证明的. ■

确定商 R/I 的另一个办法是求一个环 R' 及一个以 I 为核的同态 $\varphi:R\longrightarrow R'$. 为说明这一点，设 $\bar{R}=\mathbb{C}[x,y]/(xy)$. 这里的事实是乘积 xy 可用于求这样的映射 φ.

【4.9】命题 环$\mathbb{C}[x,y]/(xy)$同构于积环$\mathbb{C}[x]\times\mathbb{C}[y]$的由满足条件 $p(0)=q(0)$ 的元素对$(p(x),q(y))$组成的子环.

证明 容易确定环$\mathbb{C}[x,y]/(y)$，这是因为主理想(y)是使 $y\rightsquigarrow 0$ 的代入同态 $\varphi:\mathbb{C}[x,y]\longrightarrow\mathbb{C}[x]$的核. 由第一同构定理，$\mathbb{C}[x,y]/(y)\approx\mathbb{C}[x]$. 类似地，$\mathbb{C}[x,y]/(x)\approx\mathbb{C}[y]$. 因而自然会看到由 $f(x,y)\rightsquigarrow(f(x,0),f(0,y))$定义的积环的同态 $\varphi:\mathbb{C}[x,y]\longrightarrow\mathbb{C}[x]\times\mathbb{C}[y]$. φ 的核是两个核的交：$\ker\varphi=(y)\cap(x)$. 一个多项式要属于这个交，它必须同时被 y 和 x 整除. 这正说明它可被 xy 整除. 所以 $\ker\varphi=(xy)$. 由第一同构定理，$\bar{R}=\mathbb{C}[x,y]/(xy)$同构于同态 φ 的象. 该象是命题陈述中所描述的子环. ■

363

除了第一同构定理，没有确定商环的一般方法，因为它通常不是一个熟悉的环. 例如环$\mathbb{C}[x,y]/(y^2-x^3+x)$是一个与我们至今所见到的环基本上都不同的环.

第五节 元素的添加

本节讨论与关系的引入密切相关的一个过程，也就是在一个环上添加新元素的过程. 这一过程的模型是从实数构造复数域的过程. 在$\mathbb{R}$中加上 i 得到$\mathbb{C}$的这个构造完全是形式的. 即虚数 i 除了由关系

【5.1】
$$\mathrm{i}^2=-1$$

所强加的性质外没有别的性质．我们现在要理解这一构造背后的一般原理．从任意一个环 R 开始，考虑构造一个包含 R 的元素同时包含一个记为 α 的新元素的更大的环．我们希望 α 满足一个例如像(5.1)一样的关系．一个包含环 R 为其子环的环 R' 称为 R 的一个**环扩张**．因而我们是在寻找适当的环扩张．

有时元素 α 会在一个已知的环扩张 R' 中．在这种情形，解是 R' 中由 R 和 α 生成的子环．这个子环记作 $R[\alpha]$．当 $R=\mathbb{Z}$ 和 $R'=\mathbb{C}$ 时我们已在第一节描述了这个环．一般情形的描述没有什么区别：$R[\alpha]$ 由 R' 中系数 r_i 属于 R 的多项式表达式

$$r_n\alpha^n+\cdots+r_1\alpha+r_0$$

组成．但正如第一次由 $\mathbb{R}$ 构造 $\mathbb{C}$ 时所发生的一样，我们也许还不知道一个含有 α 的扩张．于是必须抽象地构造它．实际上，我们在构造多项式环 $R[x]$ 时就已经这样做了．

注意多项式环 $R[x]$ 是 R 的扩张，且它由 R 和 x 生成．因而记号 $R[x]$ 与上面引入的记号是一致的．而且代入原理(3.4)告诉我们多项式环是我们的添加一个新元素的问题在下面的意义下**普遍的解**：如果 α 是 R 的任意环扩张 R' 中的任一元素，则存在唯一的映射 $R[x]\longrightarrow R'$，它在 R 上是恒等映射且将 x 映到 α．这个映射的象是子环 $R[\alpha]$．

考虑我们的新元素所希望满足的关系这一问题．多项式环 $R[x]$ 的变量 x 除了如 $0x=0$ 那样由环的公理所蕴涵的关系外，不满足别的关系．这是表述多项式环泛性质的另一个方法．可能需要一些非平凡关系．但是既然有了多项式环 $R[x]$，就可以用第四节给出的过程，在它上面加上我们所想要的关系．通过利用多项式环 $R[x]$ 上的商构造引入关系．在构造中用 $R[x]$ 代替 R 使得记号变得复杂，但除了记号复杂一点外，没有什么不同．

364

例如，可以通过在实多项式环 $\mathbb{R}[x]=P$ 上引入关系 $x^2+1=0$ 形式地构造复数．为此构造商环 $\overline{P}=P/(x^2+1)$．x 的剩余成为我们的元素 i．注意在 $\overline{P}$ 中关系 $\overline{x^2+1}=\bar{x}^2+\bar{1}=0$ 成立，因为映射 π：$P\longrightarrow\overline{P}$ 是同态且 $x^2+1\in\ker\pi$．由于 $\bar{1}$ 是 $\overline{P}$ 的单位元，而我们的单位元的标准记号上面不用横线．因而 $\overline{P}$ 由在 $\mathbb{R}$ 上加上满足条件 $\bar{x}^2+1=0$ 元素 $\bar{x}$ 得到．换言之，$P\approx\mathbb{C}$，这正是所要求的．

$\mathbb{R}[x]/(x^2+1)$ 同构于 $\mathbb{C}$ 这一事实亦可由第一同构定理(4.2b)得到：用 i 代替 x(3.4)定义一个满同态 φ:$\mathbb{R}[x]\longrightarrow\mathbb{C}$，其核是以 i 为根的实多项式的集合．如果 i 是一个实多项式 $p(x)$ 的根，则 $-$i 也是一个根．因而 $x-$i 和 $x+$i 都整除 $p(x)$．核是由能被 $(x-\mathrm{i})(x+\mathrm{i})=x^2+1$ 整除的多项式组成的集合，它是主理想 (x^2+1)．由第一同构定理，$\mathbb{C}$ 同构于 $\mathbb{R}[x]/(x^2+1)$．

第八章第六节用到了添加一个元素的另一个简单例子，其中引入了满足条件

【5.2】
$$\varepsilon^2=0$$

的形式无穷小元素来计算切向量．环 R 的一个元素称为**无穷小的**或**幂零的**，如果它的某个幂为零，我们的过程使得能在一个环上添加一个无穷小元．这样添加一个满足条件(5.2)的元素 ε 到一个环 R 的结果是商环 $R'=R[x]/(x^2)$．x 的剩余是无穷小元素 ε．在这个环中，关系 $\varepsilon^2=0$ 将所有 ε 的多项式表达式化为次数 <2 的多项式，这样 R' 的元素具有 $a+b\varepsilon$ 的形式，其中 a，$b\in R$. 但其乘法规则[第八章(6.5)]与复数乘法的规则是不同的．

一般地，如果想要在环 R 上添加一个满足一个或多个形如

【5.3】
$$f(\alpha)=c_n\alpha^n+\cdots+c_1\alpha+c_0=0$$

的多项式关系的元素 α，则其解是 $R'=R[x]/I$，其中 I 是 $R[x]$ 的由多项式 $f(x)$ 生成的理想. 如果 α 表示 x 在 R' 中的剩余 $\bar{x}$，则

【5.4】
$$0=\overline{f(x)}=\bar{c}_n\bar{x}^n+\cdots+\bar{c}_0=\bar{c}_n\alpha^n+\cdots+\bar{c}_0.$$

这里 $\bar{c}_i$ 是常数多项式 c_i 在 R' 中的象. 因而 α 满足 R' 中对应于 R 中关系(5.3)的关系. 这样得到的环常表示为

【5.5】
$$R[\alpha]=\text{将 }\alpha\text{ 添加到 }R\text{ 上得到的环}.$$

重复这个过程可以添加多个元素 $\alpha_1,\cdots,\alpha_m$，也可以通过同时在 m 个变量的多项式环 $R[x_1,\cdots,x_m]$ 上引入适当的关系得到.

365

最重要的情形之一是要求新元素 α 满足单独一个次数 $n>0$ 的首一的方程. 假如希望关系 $f(x)=0$，其中 f 是首一多项式

【5.6】
$$f(x)=x^n+c_{n-1}x^{n-1}+\cdots+c_1x+c_0.$$

在这一特殊情形不难精确地描述环 $R[\alpha]$.

【5.7】命题 设 R 是环，并设 $f(x)$ 是系数属于 R 的具有正次数 n 的首一多项式. 设 $R[\alpha]$ 表示通过添加一个满足关系 $f(\alpha)=0$ 的元素得到的环. 存在 $R[\alpha]$ 的元素与向量 $(r_0,\cdots,r_{n-1})\in R^n$ 间的一一对应. 这样的向量对应于线性组合

$$r_0+r_1\alpha+r_2\alpha^2+\cdots+r_{n-1}\alpha^{n-1},\text{其中 } r_i\in R.$$

命题指出幂 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 构成 $R[\alpha]$ 在 R 上的基. 要在 $R[\alpha]$ 中将两个这样的多项式相乘，我们用多项式乘法，然后除以 f. 余式就是代表这个积的 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 的线性组合. 因此虽然 R' 的加法仅依赖于次数，但乘法强烈地依赖于特定的多项式 f.

例如，设 R' 由在 $\mathbb{Z}$ 上添加一个满足关系 $\alpha^3+3\alpha+1=0$ 的元素 α 得到. 因此 $R'=\mathbb{Z}[x]/(x^3+3x+1)$. R' 的元素是线性组合 $r_0+r_1\alpha+r_2\alpha^2$，其中 r_i 是整数. 两个线性组合的加法是多项式加法：例如，$(2+\alpha-\alpha^2)+(1+\alpha)=3+2\alpha-\alpha^2$. 要作乘法，我们先用多项式乘法计算其积：$(2+\alpha-\alpha^2)(1+\alpha)=2+3\alpha-\alpha^3$. 然后用 $1+3\alpha+\alpha^3$ 去除：$2+3\alpha-\alpha^3=(1+3\alpha+\alpha^3)(-1)+(3+6\alpha)$. 因为在 R' 中 $1+3\alpha+\alpha^3=0$，余数 $3+6\alpha$ 是代表积的线性组合.

或者设 R' 是由 $\mathbb{F}_5$ 上添加满足关系 $\alpha^2-3=0$ 的元素 α 得到的环，即 $R'=\mathbb{F}_5[x]/(x^2-3)$. 这里 α 表示 3 的形式平方根. R' 的元素是系数 a，$b\in\mathbb{F}_5$ 的 α 的 25 个线性表达式 $a+b\alpha$. 这个环是一个域. 为证这一点，我们验证 R' 的每个非零元素 $a+b\alpha$ 可逆. 注意 $(a+b\alpha)(a-b\alpha)=a^2-3b^2\in\mathbb{F}_5$. 而且方程 $x^2=3$ 在 $\mathbb{F}_5$ 中无解，这表明 $a^2-3b^2\neq0$. 因而 a^2-3b^2 在 $\mathbb{F}_5$ 中和 R' 中可逆. 这说明 $a+b\alpha$ 在 $\mathbb{F}_5$ 中也可逆. 其逆为 $(a^2-3b^2)^{-1}(a-b\alpha)$.

另一方面，同样的过程应用于 $\mathbb{F}_{11}$ 上却不能得到一个域. 原因是在 $\mathbb{F}_{11}[x]$ 中 $x^2-3=(x+5)(x-5)$. 因而如果 α 表示 x 在 $R'=\mathbb{F}_{11}[x]/(x^2-3)$ 中的剩余，则 $(\alpha+5)(\alpha-5)=0$. 注意到通过添加 3 的平方根到 $\mathbb{F}_{11}$ 上构造 R'，而这时域中已含有两个平方根 ±5，这样可以直观地得到解释. 读者第一个反应是会期望这一过程又得到了 $\mathbb{F}_{11}$. 但我们没说 α 等于 5 还是 -5，只是说它的平

366 方为 3. 关系$(\alpha+5)(\alpha-5)=0$反映了这种不确定性.

命题(5.7)的证明 由于$R[\alpha]$是多项式环$R[x]$的商，$R[\alpha]$的每个元素都是多项式的剩余. 这就是说它可写为$g(\alpha)$的形式，其中$g(x)\in R[x]$是个多项式. 用关系$f(\alpha)=0$可将任一次数$\geqslant n$的多项式$g(\alpha)$用一个次数较低的多项式代替：对$g(x)$应用带余除法用$f(x)$除，得到形如$g(x)=f(x)q(x)+r(x)$的表达式(3.19). 由于$f(\alpha)=0$，$g(\alpha)=r(\alpha)$. 这样$R[\alpha]$的每个元素β可写为次数$<n$的α的多项式.

我们现在证明由$f(x)$生成的主理想不包含次数$<n$的多项式，因而对每个次数$<n$的非零多项式$g(x)$有$g(\alpha)\neq 0$. 这蕴涵元素β的一个次数$<n$的表达式是唯一的. 由$f(x)$生成的主理想是f的所有倍元hf的集合. 假设$h(x)=b_mx^m+\cdots+b_0$，且$b_m\neq 0$. 则$h(x)f(x)$的最高次项为b_mx^{m+n}，因此hf的次数$m+n\geqslant n$. 这就完成了命题的证明. ■

分析由在环上添加上一个满足非首一多项式关系的元素得到的环的结构是比较困难的. 最简单和最重要的情形之一是由添加一个元素的乘法逆得到的环. 如果一个元素$a\in R$有逆α，则α满足关系

【5.8】
$$a\alpha-1=0.$$

因而可以通过构造商环$R'=R[x]/(ax-1)$而添加上一个逆. x的剩余成为a的逆α. 这个环没有命题(5.7)所描述的那一类型的基，但可以相当容易地计算它，因为R'的每个元素都有α^kr的形式，其中$r\in R$而k是非负整数：比如$\beta=r_0+r_1\alpha+\cdots+r_{n-1}\alpha^{n-1}$，其中$r_i\in R$. 于是由于$a\alpha=1$，亦可记$\beta=\alpha^{n-1}(r_0a^{n-1}+r_1a^{n-2}+\cdots+r_{n-1})$.

一个有意思的例子是R自己就是一个多项式环，比如$R=F[t]$，我们在变量t上添加逆元. 则$R'=F[t,x]/(xt-1)$. 这个环自然等同于t的洛朗多项式环$F[t,t^{-1}]$. 洛朗多项式是形如

【5.9】
$$f(t)=\sum_{-n}^{n}a_it^i=a_{-n}t^{-n}+\cdots+a_{-1}t^{-1}+a_0+a_1t+\cdots+a_nt^n$$

的t和t^{-1}的多项式. 我们将这个同构的构造留作练习.

现在必须考虑在讨论添加元素时没有提及的一个要点：当添加一个元素α到环R上并加上某些关系时，原来的环R会不会是得到的环$R[\alpha]$的子环？我们知道R作为常数多项式的子环包含在多项式环$R[x]$中. 因而典范映射π：$R[x]\longrightarrow R[x]/I=R[\alpha]$在常数多项式的限制上给

367 出一个同态ψ：$R\longrightarrow R[\alpha]$，它是前面考虑的映射$r \rightsquigarrow \bar{r}$. 原则上容易确定映射$\psi$：$R\longrightarrow R[\alpha]=R[x]/I$的核. 它是理想$I$中的常数多项式的集合：

【5.10】
$$\ker\psi=R\cap I.$$

当α所满足的是一个首一等式时，由命题(5.7)得到ψ为单射，因而$\ker\psi=0$. 但ψ并不总是单射.

例如，我们最好不要把 0 的逆添加到一个环上. 由等式$0\alpha=1$会得到$0=1$. 只有在零环中零元才是可逆的，因而如果硬要添加上 0 的逆，最后得到的必将是零环.

更一般地，设a，b是环R中使得乘积ab为零的两个元素. 则除非$b=0$，否则a不可逆. 因为如果a^{-1}在R中存在，则$b=a^{-1}ab=a^{-1}0=0$. 由此得到如果一个环R的两个元素的积ab

为 0，则将 a 的逆添加到 R 的过程必将使 b 为零．这也可直接看到：$R[x]$中由 $ax-1$ 生成的理想包含$-b(ax-1)=b$，这表明 b 在环$R[x]/(ax-1)$中的剩余为零．

例如在$\mathbb{Z}/(6)$中 $\bar{2}\cdot\bar{3}=0$．如果添加 $\bar{3}^{-1}$到这个环，就必将消灭 $\bar{2}$．消灭 $\bar{2}$ 后使$\mathbb{Z}/(6)$坍缩成为$\mathbb{Z}/(2)=\mathbb{F}_2$．由于 $\bar{3}=\bar{1}$ 在$\mathbb{F}_2$ 中可逆，没有必要进行其他作用，$R'=(\mathbb{Z}/(6))[x]/(\bar{3}x-\bar{1})\approx\mathbb{F}_2$．这亦可直接验证．为此，注意到环 R'同构于$\mathbb{Z}[x]/(6,3x-1)$，我们分析两个关系 $6=0$及 $3x-1=0$．这蕴涵 $6x=0$ 及 $6x-2=0$；因此 $2=0$．于是亦有 $2x=0$，与 $3x-1=0$ 结合起来，这表明 $x-1=0$．因此$\mathbb{Z}[x]$的理想$(6,3x-1)$包含元素$(2,x-1)$．另一方面，6 及 $3x-1$属于理想$(2,x-1)$．因而两个理想相等，且 R'同构于$\mathbb{Z}[x]/(2,x-1)\approx\mathbb{F}_2$．

环的一个元素 a 称为一个零因子，如果存在一个非零元素 b 使得 $ab=0$．例如，3 的剩余是环$\mathbb{Z}/(6)$的一个零因子．术语“零因子”是流传下来的术语，但却是个很糟糕的选择，因为实际上所有 $a\in R$ 都整除零：$0=a0$．

第六节　整环与分式域

环与域的区别是环 R 的非零元素不必有逆．本节讨论把一个给定的环作为子环嵌入到一个域的问题．上节看到不消灭某些元素就不能添加一个零因子的逆．因而包含零因子的环不能嵌入一个域．

【6.1】定义　*一个整环 R 是一个没有零因子的非零环．换言之，它具有性质：如果 $ab=0$，则 $a=0$ 或 $b=0$，并且在 R 中 $1\neq0$．*

368

例如，域的子环是整环．

整环满足消去律：

【6.2】　*如果 $ab=ac$ 且 $a\neq0$，则 $b=c$．*

因为由 $ab=ac$ 可得 $a(b-c)=0$．则由 $a\neq0$ 得到 $b-c=0$．

【6.3】命题　*设 R 是一个整环．则多项式环 $R[x]$是整环．*

【6.4】命题　*有限个元素的整环是域．*

我们把这些命题的证明留作练习．

【6.5】定理　*设 R 是一个整环．则存在 R 到一个域的嵌入，即存在一个单同态 $R\longrightarrow F$，其中 F 是域．*

我们可以用上节所描述的过程，通过在 R 上添加其所有非零元素的逆来构造域．但在这种情形中用分式来构造 F 要简单一些．我们的模型是有理数作为整数的分式的构造，而一旦有了使用分式的想法，其构造便非常严格地按照有理数的构造方式进行．

设 R 是一个整环．分式是一个符号 a/b，其中 $a,b\in R$ 且 $b\neq0$．两个分式 a_1/b_1，a_2/b_2 称为等价的，记为 $a_1/b_1\approx a_2/b_2$，如果

$$a_1b_2=a_2b_1.$$

我们检验这个关系的传递性——自反性和对称性是显见的(见第二章第五节)．假设 $a_1/b_1\approx a_2/b_2$ 并且还有 $a_2/b_2\approx a_3/b_3$．则 $a_1b_2=a_2b_1$ 且 $a_2b_3=a_3b_2$．乘上 b_3 和 b_1 得到

$$a_1b_2b_3 = a_2b_1b_3 = a_3b_2b_1.$$

消去 b_2 得到 $a_3b_1=a_1b_3$. 这样 $a_1/b_1 \approx a_3/b_3$.

R 的分式域 F 是分式的等价类的集合. 如在有理数中一样，如果分式 a_1/b_1，a_2/b_2 是等价分式，我们说它们是相等的元素：在 F 中 $a_1/b_1=a_2/b_2$ 意味着 $a_1b_2=a_2b_1$. 分式的加法和乘法如同在算术中那样定义：

$$(a/b)(c/d) = ac/bd, \quad a/b + c/d = \frac{ad+bc}{bd}.$$

这里必须验证当 a/b 和 c/d 用等价的分式代替时，由这些法则得到等价的答案. 然后还必须验证域的公理. 所有这些验证都是直接的练习.

注意如果将 $a \in R$ 等同于分式 $a/1$，则由于仅当 $a=b$ 时有 $a/1 \approx b/1$，故 R 包含在 F 中. 369 映射 $a \rightsquigarrow a/1$ 是定理中提到的单同态.

作为例子，考虑多项式环 $K[x]$，其中 K 是任意域. 这是个整环，其分式域称为系数属于 K 的 x 的有理函数域. 这个域通常记作

【6.6】 $K(x)=\{$分式 f/g 的等价类，其中 f，g 是多项式且 g 不是零多项式.$\}$

如果 $K=\mathbb{R}$，则只要 $g(x)\neq 0$，有理函数 $f(x)/g(x)$ 的取值便定义了一个实直线上真正的函数. 但与多项式一样，我们要区别由多项式的分式形式上定义的有理函数和由它们的取值定义的实际函数.

分式域是将整环嵌入到一个域的这一问题的通解. 下面的命题表明了这一点：

【6.7】命题 设 R 是一个整环，其分式域为 F，并设 $\varphi: R \longrightarrow K$ 是 R 到一个域 K 的单同态. 则规则

$$\Phi(a/b) = \varphi(a)\varphi(b)^{-1}$$

定义 φ 的唯一扩张同态 Φ：$F \longrightarrow K$.

证明 我们必须验证扩张是唯一定义的. 首先，由于分式的分母不允许为零且由于 φ 是单射，对任意分式 a/b，$\varphi(b)\neq 0$. 因而 $\varphi(b)$ 在 K 中可逆，且 $\varphi(a)\varphi(b)^{-1}$ 是 K 的一个元素. 其次，验证等价的分式有相同的象：如果 $a_2/b_2 \approx a_1/b_1$，则 $a_2b_1=a_1b_2$；因此 $\varphi(a_2)\varphi(b_1)=\varphi(a_1)\varphi(b_2)$ 且 $\Phi(a_2/b_2)=\varphi(a_2)\varphi(b_2)^{-1}=\varphi(a_1)\varphi(b_1)^{-1}=\Phi(a_1/b_1)$，这正是想要的. Φ 是同构及它是 φ 的唯一扩张的事实是容易得到的. ■

第七节 极大理想

本节讨论由一个环 R 到一个域 F 的满同态

【7.1】 $$\varphi: R \longrightarrow F.$$

给定一个这样的同态，第一同构定理告诉我们 F 同构于 $R/\ker\varphi$. 因而可以由核在相差一个同构的前提下恢复 F 与 φ. 要对这样的同态分类，必须确定使得 R/M 是域的理想 M.

由对应定理(4.3)，$\bar{R}=R/M$ 的理想与 R 中包含 M 的理想对应. 而且域由它恰有两个理想这一性质刻画(3.16). 因而如果 $\bar{R}$ 是域，则恰好有两个理想包含 M，即 M 和 R. 这样的一个理想称为极大理想.

【7.2】定义 一个理想 M 称为极大的，如果 $M\neq R$ 并且 M 不能包含在除了 M 与 R 以外的任意理想之中.

370

【7.3】推论

(a) 环 R 的一个理想 M 是极大的当且仅当 $\overline{R}=R/M$ 是一个域.

(b) R 的零理想极大当且仅当 R 是一个域.

下面的命题由 $\mathbb{Z}$ 的所有理想都是主理想这一事实得到.

【7.4】命题 整数环 $\mathbb{Z}$ 的极大理想是由素整数生成的主理想.

一个变量的复多项式环 $\mathbb{C}[x]$ 的极大理想可以非常简单地描述：

【7.5】命题 多项式环 $\mathbb{C}[x]$ 的极大理想是由线性多项式 $x-a$ 生成的主理想. 由 $x-a$ 生成的理想 M_a 是使得 $f(x)\rightsquigarrow f(a)$ 的代入同态 s_a：$\mathbb{C}[x]\longrightarrow\mathbb{C}$ 的核. 因而存在一个极大理想 M_a 和复数 a 之间的一一对应.

证明 先证明每一个极大理想是由线性多项式 $x-a$ 生成的. 设 M 是极大理想. 由命题(3.21)，M 是由一个次数最低的首一多项式 $f\in M$ 生成的主理想. 由于每一个正次数复多项式有一个根，f 被某个线性多项式 $x-a$ 整除. 于是 f 属于主理想 $(x-a)$，因此 $M\subset(x-a)$. 由于 M 是极大理想，$M=(x-a)$.

其次，证明代入同态 s_a 的核由 $x-a$ 生成：说多项式 g 在 s_a 的核中等于说 a 是 g 的根，或者 $(x-a)$ 整除 g. 这样 $(x-a)$ 生成 $\ker s_a$. 由于 s_a 的象是域，这也说明 $(x-a)$ 是极大理想. ■

命题(7.5)在多个变量的拓广是关于多项式环最重要的定理之一.

【7.6】定理 希尔伯特零点定理：多项式环 $\mathbb{C}[x_1,\cdots,x_n]$ 的极大理想与复 n 维空间的点一一对应. $\mathbb{C}^n$ 的一个点 $a=(a_1,\cdots,a_n)$ 对应于使得 $f(x)\rightsquigarrow f(a)$ 的代入映射 s_a：$\mathbb{C}[x_1,\cdots,x_n]\longrightarrow\mathbb{C}$ 的核. 这个映射的核 M_a 是由线性多项式

$$x_1-a_1,\cdots,x_n-a_n$$

生成的理想.

证明 设 $a\in\mathbb{C}^n$ 而 M_a 是代入映射 s_a 的核. 由于 s_a 是满射且 $\mathbb{C}$ 是域，因此 M_a 是极大理想. 其次证明 M_a 如断言中所述是由线性多项式生成的. 为此，将 $f(x)$ 按 $x_1-a_1,\cdots,x_n-a_n$ 的幂展开，记

371

$$f(x)=f(a)+\sum_i c_i(x_i-a_i)+\sum_{i,j}c_{ij}(x_i-a_i)(x_j-a_j)+\cdots.$$

你也许认出这是泰勒展开式：$c_i=\partial f/\partial x_i$，等等. 这个展开式的存在性可以用代数的方法导出：将 $x=u+a$ 代入 f，展开成为变量 u 的幂，再将 $u=x-a$ 代回到结果中. 注意除了 $f(a)$ 以外右边的每一项可以被多项式 x_i-a_i 中的至少一个整除. 因而如果 f 属于 s_a 的核，即如果 $f(a)=0$,则 $f(x)$ 属于这些元素生成的理想. 这表明多项式 x_i-a_i 生成 M_a.

证明存在某个点 $a\in\mathbb{C}^n$，使得每个极大理想具有 M_a 的形式是比较困难的. 为此，设 M 是任意极大理想，并用 K 表示域 $\mathbb{C}[x_1,\cdots,x_n]/M$. 考虑典范映射(4.1)$\pi$：$\mathbb{C}[x_1,\cdots,x_n]\longrightarrow K$ 在一元多项式环 $\mathbb{C}[x_1]$ 上的限制：

$$\pi_1:\mathbb{C}[x_1]\longrightarrow K.$$ ■

【7.7】引理 π_1 的核或为 0 或是极大理想.

证明 假设核不为零，并设 f 是 $\ker\pi_1$ 中的一个非零元素. 由于 K 不是零环，$\ker\pi_1$ 不是

整个环. 因而 f 不是常数，这表明它能被线性多项式整除，比如 $f=(x_1-a_1)g$. 于是在 K 中 [370] 有$\pi_1(x_1-a_1)\pi_1(g)=\pi_1(f)=0$. 由于 K 是域，$\pi_1(x_1-a_1)=0$ 或 $\pi_1(g)=0$. 因而两个元素 x_1-a_1 或 g 之一属于 $\ker\pi_1$. 对 f 的次数作归纳，得 $\ker\pi_1$ 含有一个线性多项式. 因此它是一个极大理想(7.5). ■

我们要证明 $\ker\pi_1$ 不是零理想. 由此将得到 M 中含有一个形如 x_1-a_1 的线性多项式. 由于指标 1 可以由任意的指标代替，对每个 $\nu=1, \cdots, n$, M 中包含形如 $x_\nu-a_\nu$ 的多项式. 正如我们所断言的，这表明 M 包含在(因而也就等于)代入映射 $f(x)\rightsquigarrow f(a)$的核中.

假设 $\ker\pi_1=(0)$. 则 π_1 将$\mathbb{C}[x_1]$同构地映到其象之上，这是 K 的子环. 由命题(6.7)，这个映射可以扩张成为$\mathbb{C}[x]$的分式域上的同态. 因此 K 包含一个同构于有理函数域$\mathbb{C}(x)$的域[见(3.17)].

单项式 $x^i=x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ 构成$\mathbb{C}[x_1, \cdots, x_n]$的作为$\mathbb{C}$上向量空间的基. 这样$\mathbb{C}[x_1, \cdots, x_n]$有一个可数基(附录，第一节). 由于 K 是$\mathbb{C}[x_1, \cdots, x_n]$的商，存在一个可数的元素簇在$\mathbb{C}$上作为向量空间张成 K，也就是单项式的剩余张成这个域. 我们将证明$\mathbb{C}(x)$中有不可数多个线性无关的元素. 由此将得到[引理(7.9)]$\mathbb{C}(x)$不能同构于 K 的子空间. 这个矛盾表明 $\ker\pi_1\neq(0)$.

我们所需要的事实是复数域$\mathbb{C}$的元素不能构成一个可数集合[附录(1.7)]. 利用这个事实，下面两个引理将完成我们的证明：

[372] **【7.8】引理** 不可数多个有理函数$(x-\alpha)^{-1}(\alpha\in\mathbb{C})$是线性无关的.

证明 通过在复平面所有满足 $g\neq0$ 的点取值，一个有理函数 f/g 定义一个实际的函数. 有理函数$(x-\alpha)^{-1}$在 α 处有一个极点，这意味着它在 α 附近取任意大的值. 而它在其他任意点附近是有界的. 考虑线性组合

$$\sum_{i=1}^{n}\frac{c_i}{x-\alpha_i},$$

其中 $\alpha_1, \cdots, \alpha_n$ 是不同的复数，且其中某个系数(比如说 c_1)是非零的. 这个和式中的第一项在 α_1 附近是无界的，但其他项在那里有界. 由此线性组合所定义的不是零函数；因此它不为零. ■

【7.9】引理 设 V 是由向量的可数簇$\{v_1, v_2, \cdots\}$张成的向量空间. 则 V 的每个线性无关的向量集合 L 是有限的或可数无限的.

[371] **证明** 设 L 是 V 的一个线性无关的子集，设 V_n 是由前 n 个向量 $v_1, \cdots, v_n$ 张成的向量空间，并设 $L_n=L\cap V_n$. 则 L_n 是一个有限维向量空间 V_n 中的线性无关的集合，因而它是有限集[第三章(3.16)]. 而且 L 是所有 L_n 的并. 可数多个有限集的并是有限的或可数无限的. ■

第八节 代数几何

代数几何对我来说是令人激动的代数.

Solomon Lefschetz

设 V 是复 n-空间$\mathbb{C}^n$ 的一个子集. 如果 V 可以定义为有限多个 n 个变量的多项式的公共零点的集合，则把它称为代数簇，或简称为簇. (我不知道这个不吸引人的术语的由来.)例如，

根据定义，$\mathbb{C}^2$ 中的复直线是线性方程 $ax+by+c=0$ 的解的集合．这是一个簇．一个点也是一个簇．点 (a, b) 是两个多项式 $x-a$ 与 $y-b$ 的公共零点的集合．我们已经见到不少其他有意思的簇．例如群 $SL_2(\mathbb{C})$，作为多项式方程 $x_{11}x_{22}-x_{12}x_{21}-1=0$ 的解的轨迹，是 $\mathbb{C}^4$ 中的簇．

希尔伯特零点定理为我们提供了代数与几何间的重要联系．它告诉我们多项式环 $\mathbb{C}[x]=\mathbb{C}[x_1, \cdots, x_n]$ 的极大理想对应于 $\mathbb{C}^n$ 的点．这个对应也可用来将代数簇与多项式环的商环联系起来．

【8.1】定理 *设 $f_1, \cdots, f_r$ 是 $\mathbb{C}[x_1, \cdots, x_n]$ 中的多项式，并设 V 是由方程组 $f_1(x)=0, \cdots, f_r(x)=0$ 定义的簇．设 I 是由给定的多项式生成的理想 $(f_1, \cdots, f_r)$．商环 $R=\mathbb{C}[x]/I$ 的极大理想与 V 中的点一一对应．*

373

证明 R 的极大理想对应于 $\mathbb{C}[x]$ 中包含 I 的那些极大理想[对应定理(4.3)]．而一个理想包含 I 当且仅当它包含 I 的生成元 $f_1, \cdots, f_r$．另一方面，对应于一个点 $a\in\mathbb{C}^n$ 的极大理想 M_a 是代入映射 $f(x) \rightsquigarrow f(a)$ 的核．因而 $f_i\in M_a$ 当且仅当 $f_i(a)=0$，这表明 $a\in V$． ■

定理指出环 R 的代数性质与 V 的几何是紧密相关的．原则上多项式方程组

【8.2】
$$f_1(x)=\cdots=f_r(x)=0$$

的所有性质都反映在环 $R=\mathbb{C}[x]/(f_1, \cdots, f_r)$ 的结构上．这一关系的理论是称为代数几何的数学领域．在这里不会花时间在其中走得太远．我们要学习的重要的东西是簇的几何性质提供了关于环的信息，反过来也一样．

关于集合的最简单的问题是它是否是空集．因而我们会问一个环是否可能根本没有极大理想．答案是这只有对零环才会发生：

【8.3】定理 *设 R 是一个环．R 的每个不是单位理想的理想包含在一个极大理想之中．*

【8.4】推论 *没有极大理想的环 R 只有零环．*

定理(8.3)可用选择公理或佐恩引理来证明．然而对于多项式环的商环它是希尔伯特基定理的结果，我们将在后面[第十二章(5.18)]证明它．为了避免对选择公理的讨论，我们将其证明推迟到第十二章．

如果把定理(8.1)和(8.3)放在一起，将得到另一个重要的推论：

【8.5】推论 *设 $f_1, \cdots, f_r$ 是 $\mathbb{C}[x_1, \cdots, x_n]$ 中的多项式．如果方程组 $f_1=\cdots=f_r=0$ 在 $\mathbb{C}^n$ 中无解，则 1 是 f_i 具有多项式系数的线性组合*

$$1=\sum g_i f_i.$$

因为如果方程组无解，则定理(8.1)告诉我们不存在包含理想 $I=(f_1, \cdots, f_r)$ 的极大理想．由定理(8.3)，I 是单位理想．

374

有两个变量 x, y 的三个多项式 f_1, f_2, f_3 的大多数选择没有公共解．由此通常可以把 1 表示为线性组合 $1=p_1f_1+p_2f_2+p_3f_3$，其中 p_i 是多项式．这并不明显．例如，由

【8.6】
$$f_1=x^2+y^2-1, f_2=x^2-y+1, f_3=xy-1$$

生成的理想是单位理想．这可以通过验证 $f_1=f_2=f_3=0$ 在 $\mathbb{C}^2$ 中无解来证明．如果没有零点定理，则要花点时间才能发现可以把 1 写成这三个多项式的多项式系数的线性组合．

零点定理已经被以多种方式重新叙述，实际上上节所给出的并不是它的原始形式．它的原

始形式是：

【8.7】定理　零点定理的经典形式：设 $f_1, \cdots, f_r$ 和 g 是 $\mathbb{C}[x_1, \cdots, x_n]$ 中的多项式. 设 V 是 $f_1, \cdots, f_r$ 的零点的簇，并设 I 是由这些多项式生成的理想. 如果 $g=0$ 在 V 上恒成立，则 g 的某个幂属于理想 I.

证明　为证明这一点，我们研究由多项式 g 通过方程 $gy=1$ 取逆得到的环. 假设 g 在 V 上恒为零. 考虑变量 $x_1, \cdots, x_n, y$ 的 $r+1$ 个多项式 $f_1(x), \cdots, f_r(x), g(x)y-1$. 只有最后一个是涉及变量 y 的多项式. 注意到这些多项式在 C^{n+1} 中没有公共零点. 因为如果 $f_1, \cdots, f_r$ 在一个点 $(a_1, \cdots, a_n, b)\in C^{n+1}$ 上为零，则由假设 g 亦为零，从而 $gy-1$ 取值为 -1. 推论(8.5)告诉我们多项式 $f_1, \cdots, f_r, gy-1$ 在 $\mathbb{C}[x, y]$ 中生成单位理想. 因而可以记

$$1=\sum_i p_i(x,y)f_i(x,y)+q(x,y)(g(x)y-1).$$

将 $y=1/g$ 代入这个等式，得到

$$1=\sum_i p_i(x,g^{-1})f_i(x).$$

等式两边乘上一个 g 的足够大的幂，消去 $p_i(x, g^{-1})$ 的分母. 这就得到所需要的多项式表达式

$$g(x)^N=\sum_i h_i(x)f_i(x),$$

其中 $h_i(x)=g(x)^N p_i(x, g^{-1})$. ■

对于 $\mathbb{C}^n$ 的簇想要有很好的感觉是不容易的，但是对 $\mathbb{C}^2$ 中簇的一般形状可以有一个相当简单的描述.

375

【8.8】命题　两个非零的二元多项式 $f(x, y)$，$g(x, y)$ 除非有非常数的公共因式，否则它们只有有限多个公共零点.

如果 f 和 g 的次数分别为 m 和 n，则其公共零点的个数以 mn 为界. 这称为贝祖界. 例如，两个圆锥曲线最多交于四个点. 除了有限性外要证明贝祖界是困难的，我们将不给出证明.

命题(8.8)的证明　假设 f 和 g 没有非常数的公因式. 用 F 表示 x 的有理函数域，即环 $\mathbb{C}[x]$ 的分式域. 把 f 和 g 视为一个变量的多项式环 $F[y]$ 的元素是很有用的，因为可以使用 $F[y]$ 的每个理想是主理想这一事实. 用 I 表示由 f, g 在 $F[y]$ 中生成的理想. 这是一个主理想，由 f 和 g 在 $F[y]$ 中的最大公因式 h 生成(3.22). 如果 f 和 g 在 $F[y]$ 中没有非常数公因式，则 I 是单位理想.

我们的假设是 f 和 g 在 $\mathbb{C}[x, y]$ 中没有公因式，而不是它们 $F[y]$ 中没有公因式，因而需要将这两个性质联系起来. 多项式的因子分解是下一章的主题，因而在这里只陈述需要的事实而推迟其证明(见第十一章(3.9)).

【8.9】引理　设 $f, g\in\mathbb{C}[x, y]$，并设 F 是 x 的有理函数域. 如果 f 和 g 在 $F[y]$ 中有一个不是 F 的元素的公因式，则它们在 $\mathbb{C}[x, y]$ 中有非常数公因式.

回到命题的证明. 由于两个多项式 f 和 g 在 $\mathbb{C}[x, y]$ 中没有非常数公因式，它们在 $F[y]$ 中互素，因而它们在 $F[y]$ 中生成的理想 I 为单位理想. 这样可以记 $1=rf+sg$，其中 r, s 是 $F[y]$ 中的元素. 于是 r, s 以单独一个 x 的多项式为其分母，可以在等式两边乘上一个适当的多项式 $p(x)$ 而消去分母. 这就得到形如

$$p(x)=u(x,y)f(x,y)+v(x,y)g(x,y)$$

的等式，其中 u，$v\in\mathbb{C}[x, y]$. 由这个等式得到 f 和 g 的公共零点也必是 p 的一个零点. 但 p 是单独一个 x 的多项式，而一个变量的多项式仅有有限多个根. 这样变量 x 在 f，g 的公共零点仅能取有限多个值. 同样的讨论对变量 y 也成立. 由此可得公共零点构成有限集. ■

这个命题表明$\mathbb{C}^2$ 中最有意思的簇是由单独一个多项式 $f(x, y)$的零点所定义的那些簇. 这些轨迹称为代数曲线或黎曼曲面，它们的几何可以是相当微妙的. 一个黎曼曲面是二维的，称之为代数曲线似乎是不恰当的命名. 术语曲线的使用指的是在一个点的附近，这样一个轨迹可以用一个复参数解析地描述这样一个事实.

当 f 既约时，有这样一个簇的粗略描述.（一个多项式称为既约的，如果它不能写为两个非常数多项式的乘积.）我们将 $f(x, y)$视为系数为 x 的多项式的 y 的多项式，比如

376

【8.10】
$$f(x,y)=u_n(x)y^n+\cdots+u_1(x)y+u_0(x),$$
其中 $u_i(x)\in\mathbb{C}[x]$.

【8.11】命题 设 $f(x, y)$是$\mathbb{C}[x, y]$中的既约多项式且不是一个变量 x 的多项式，并设 S 是 f 在$\mathbb{C}^2$ 的零点的轨迹. 用 n 表示 f 作为 y 的多项式的次数.

(a) 对变量 x 的每个取值 a，S 最多有 n 个点的 x-坐标为 a.

(b) 存在 x 的值的有限集合 Δ，使得当 $a\notin\Delta$ 时，S 中恰好有 n 个点的 x-坐标为 a.

证明 设 $a\in\mathbb{C}$ 并考虑多项式 $f(a, y)$. 点$(a, b)\in S$ 是那些使 b 是 $f(a, y)$的根的点. 这个多项式不是恒等于零的，因为如果它恒等于零，则 $x-a$ 将整除每个系数 $u_i(x)$，因此它将整除 f. 但由假设 f 是既约的. 其次，$f(a, y)$关于 y 的次数最多为 n，因而它最多有 n 个根. 如果要么

【8.12】

(i) $f(a, y)$的次数小于 n，要么

(ii) $f(a, y)$的次数为 n，但这个多项式有个重根，

则它的根少于 n 个.

情形(i)当首项系数 $u_n(x)$在 a 处消失，即当 a 是 $u_n(x)$的根时出现. 由于 u_n 是 x 的多项式，最多有有限多个这样的值.

一个复数 b 是多项式 $h(y)$的重根[意为$(y-b)^2$ 整除 $h(y)$]当且仅当它同时是 $h(y)$及其导数 $h'(y)$的根. 这一事实的证明留作练习. 在我们的情形，$h(y)=f(a, y)$. 第一个变量是不变的，因而导数是关于第二个变量的偏导数. 这样情形(ii)在 f 与$\partial f/\partial y$ 的公共零点(a, b)处出现. 注意 f 不能整除偏导数$\partial f/\partial y$，因为偏导数关于 y 的次数是 $n-1$，它比 f 关于 y 的次数小. 由于假设 f 是既约的，f 与$\partial f/\partial y$ 无非常数公因式. 命题(8.8)告诉我们只有有限多个公共根. ■

命题(8.11)可总结为 S 是复 x-平面 P 的一个 n-叶覆盖. 由于存在有限集 Δ，在其上 S 的叶数少于 n，它称为一个分支覆盖. 例如，考虑轨迹 $x^2+xy^2-1=0$. 这个方程对于除了 $x=0$，±1 的每一 x 的值，y 有两个解. 当 $x=0$ 时无解，当 $x=1$ 或 -1 时只有一个解. 因而这个轨迹是 P 的二重分支覆盖.

下面是分支覆盖的精确定义：

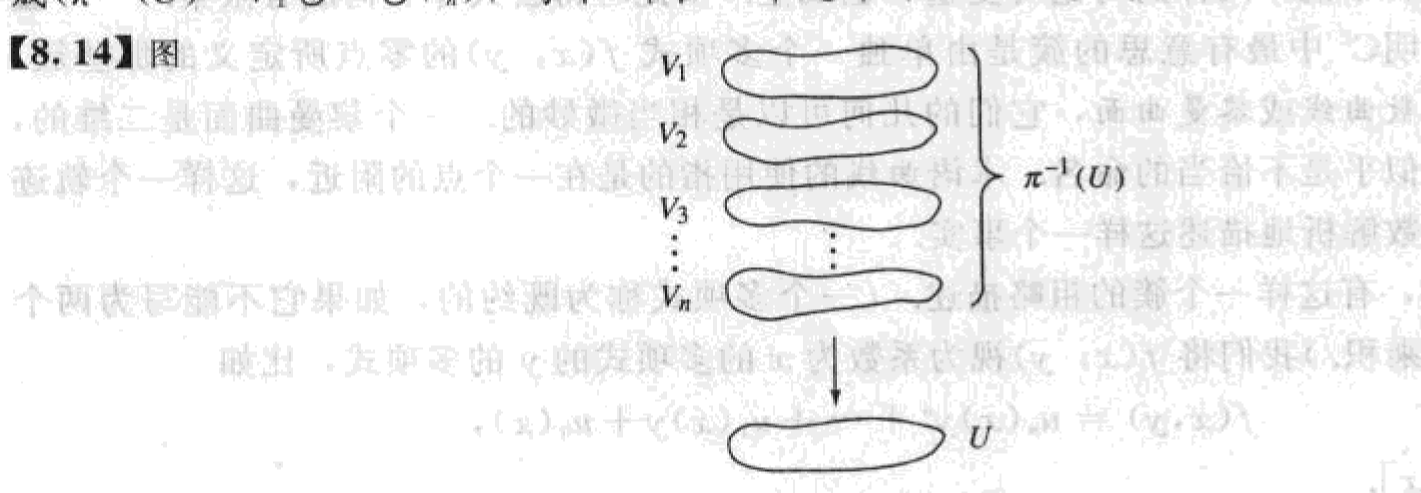
377

【8.13】定义 复平面 P 的一个 n-页分支覆盖是一个拓扑空间 S 及一个连续映射 π：$S\longrightarrow P$，满足

(a) 在 P 的一个有限集合 Δ 的补集上 π 是 n 对一的.

(b) 对每个点 $x_0\in P-\Delta$，存在 x_0 的一个开邻域 U 使得 $\pi^{-1}(U)$ 由 n 个互不连通的部分构成($\pi^{-1}(U)=V_1\cup\cdots\cup V_n$)，每个 V_i 在 S 中是开的，且 π 将 V_i 同胚地映到 U 上.

【8.14】 图



n-叶覆盖的一部分

【8.15】推论 设 $f(x, y)$ 是 $\mathbb{C}[x, y]$ 中变量 y 的次数为 $n>0$ 的既约多项式. 则 $f(x, y)$ 的黎曼曲面是平面的一个 n-页分支覆盖.

证明 f 的黎曼曲面具有分支覆盖的第一个性质这一事实是命题(8.11). 因而还要验证性质(8.13b). 考虑一个使 $f(x_0, y)$ 有 n 个根 $y_1, \cdots, y_n$ 的点 x_0. 则由于 y_1 不是 $f(x_0, y)$ 的重根，$(\partial f/\partial y)(x_0, y_1)\neq 0$. 隐函数定理[附录(4.1)]告诉我们在 x_0 的某个邻域 U 由方程(8.2)解出 $y=\alpha_1(x)$ 为 x 的连续函数，并且使得 $y_1=\alpha_1(x_0)$. 同样可以解出 $y=\alpha_i(x)$，使得 $y_i=\alpha_i(x_0)$. 减小 U 的大小，可假设每一 $\alpha_i(x)$ 在 U 上有定义. 由于所有的 $y_1, \cdots, y_n$ 互不相等而 $\alpha_i(x)$ 为连续函数，当 U 取得足够小时它们没有公共值.

考虑 n 个连续函数 α_i 的图：

【8.16】
$$V_i=\{(x,\alpha_i(x))\mid x\in U\}.$$

由于在 U 中 $\alpha_i(x)$ 没有公共值，故它们是互不相交的. 映射 $V_i\longrightarrow U$ 是同胚，因为它有连续逆函数 $U\rightsquigarrow V_i$. 这个逆函数使得 $x\rightsquigarrow(x, \alpha_i(x))$. 因为 S 在任一 x 上面最多有 n 个点，且 n 个点已被展示为 $(x, \alpha_i(x))\in V_i$，所以

$$\pi^{-1}(U)=V_1\cup\cdots\cup V_n.$$

[378] 因为集合 V_i 是连续函数 $y-\alpha_i(x)$ 的零点集，它们中的每一个都在 $U\times\mathbb{C}$ 中闭. 于是 V_i 亦在 $U\times\mathbb{C}$ 的子集 $\pi^{-1}(U)$ 中闭. 由此得 V_1 在 $\pi^{-1}(U)$ 中是开的，因为它是闭集 $V_2\cup\cdots\cup V_n$ 的补集. 由于 U 在 $\mathbb{C}$ 中是开的，其逆象 $\pi^{-1}(U)$ 在 S 中也是开的. 这样 V_i 是 S 的一个开子集中的开集，这表明 V_1 亦在 S 中为开集. 同样地，对每一 i，V_i 是开集. ■

我们将在第十三章中再来看这些轨迹.

在帮助几何的同时，
近世代数首先帮助了自己.

Oscar Zariski

练　习

第一节　环的定义

1. 在任意环 R 中证明下列恒等式.

   (a) $0a=0$　(b) $-a=(-1)a$　(c) $(-a)b=-(ab)$

2. 具体描述复数中包含 2 的实立方根的最小子环.

3. 设 $\alpha=\frac{1}{2}i$. 证明$\mathbb{Z}[\alpha]$的元素构成复平面的一个稠密子集.

4. 证明 $7+\sqrt[3]{2}$和$\sqrt{3}+\sqrt{-5}$是代数数.

5. 证明对所有整数 n，$\cos(2\pi/n)$是代数数.

6. 设$\mathbb{Q}[\alpha,\beta]$表示$\mathbb{C}$中包含$\mathbb{Q}$，$\alpha=\sqrt{2}$和$\beta=\sqrt{3}$的最小子环，并令 $\gamma=\alpha+\beta$. 证明$\mathbb{Q}[\alpha,\beta]=\mathbb{Q}[\gamma]$.

7. 设 S 是$\mathbb{R}$ 的一个在第五章(4.3)意义下为离散集合的子环. 证明 $S=\mathbb{Z}$.

8. 在下面每一情形，确定 S 是否是 R 的一个子环.

   (a) S 是所有形如 a/b 的有理数的集合，其中 b 不能被 3 整除而 $R=\mathbb{Q}$.

   (b) S 是函数$\{1, \cos nt, \sin nt \mid n\in\mathbb{Z}\}$的线性组合的函数的集合，$R$ 是所有函数$\mathbb{R}\longrightarrow\mathbb{R}$ 的集合.

   (c) (非交换)S 是形如$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$的实矩阵集合而 R 是所有实 2×2 矩阵的集合.

9. 在下面每一情形，确定给定的结构是否构成环. 如果不是环，确定哪些环的公理成立，哪些不成立.

   (a) U 是任意集合，R 是 U 的子集的集合. R 的元素的加法和乘法由规则 $A+B=A\cup B$ 和 $A\cdot B=A\cap B$ 定义.

   (b) U 是任意集合，R 是 U 的子集的集合. R 的元素的加法和乘法由规则 $A+B=(A\cup B)-(A\cap B)$和 $A\cdot B=A\cap B$ 定义.

   (c) R 是连续函数$\mathbb{R}\longrightarrow\mathbb{R}$ 的集合. 加法和乘法由规则$[f+g](x)=f(x)+g(x)$和$[f\circ g](x)=f(g(x))$定义.

10. 确定所有包含零环为其子环的环.

11. 描述每个环的单位群.

    (a) $\mathbb{Z}/12\mathbb{Z}$　(b) $\mathbb{Z}/7\mathbb{Z}$　(c) $\mathbb{Z}/8\mathbb{Z}$　(d) $\mathbb{Z}/n\mathbb{Z}$

12. 证明高斯整数环的单位为$\{\pm1, \pm i\}$.

13. 环 R 的一个元素 x 称为幂零的，如果 x 的某个幂为零. 证明如果 x 幂零，则 $1+x$ 是 R 的单位.

14. 证明具有分量加法和乘法

$$(a,a')+(b,b')=(a+b,a'+b') \quad 及 \quad (a,a')(b,b')=(ab,a'b')$$

    的两个环的积集 $R\times R'$是一个环. 这个环称为积环.

379

第二节　整数和多项式的形式构造

1. 证明除了 1 以外的每个自然数 n 对某个自然数 m 具有 m'的形式.

2. 对自然数证明下列定律.

   (a) 加法交换律.

   (b) 乘法结合律.

   (c) 分配律.

   (d) 加法消去律：如果 $a+b=a+c$，则 $b=c$.

(e) 乘法消去律：如果 $ab=ac$，则 $b=c$.

3. N 上的关系 $<$ 可由下列规则定义：如果对某个 n 有 $b=a+n$，则 $a<b$. 假定加法的初等性质已被证明.

(a) 证明如果 $a<b$，则对所有 n 有 $a+n<b+n$.

(b) 证明关系 $<$ 是传递的.

(c) 证明如果 a，b 是自然数，则下列关系中有且仅有一个成立：

$$a<b, a=b, b<a.$$

(d) 证明如果 $n\neq 1$，则 $a<an$.

4. 证明完全归纳法原理：设 S 是N的具有下列性质的子集：如果 n 是自然数使得对所有 $m<n$ 有 $m\in S$，则 $n\in S$. 那么有 $S=$N.

*5. 用N的两个复制及一个代表 0 的元素定义所有整数的集合Z，定义加法和乘法，并由自然数的加法和乘法性质推导出Z是一个环.

6. 设 R 是环. 形式幂级数 $p(t)=a_0+a_1t+a_2t^2+\cdots$(其中 $a_i\in R$)的集合构成一个通常记作 $R[[t]]$ 的环(形式幂级数意为不要求收敛性.)

(a) 证明形式幂级数构成一个环.

(b) 证明幂级数 $p(t)$ 可逆当且仅当 a_0 是 R 的单位.

7. 证明多项式环R$[x]$的单位是非零常数多项式.

第三节 同态与理想

1. 证明环同构 $\varphi: R\longrightarrow R'$ 的逆是一个同构.

2. 证明或推翻：如果一个理想含有一个单位，则它是单位理想.

380 3. 对什么整数 n 在Z$/n$Z$[x]$中 x^2+x+1 整除 $x^4+3x^3+x^2+6x+10$?

4. 证明在环Z$[x]$中，$(2)\cap(x)=(2x)$.

5. 证明理想的两个定义(3.11)和(3.12)等价.

6. 满足 2^{k+1} 整除 a_k 的多项式 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 的集合是否是Z$[x]$的理想?

7. 证明高斯整数环的每一个非零理想含有一个非零整数.

8. 描述下列映射的核.

(a) 由 $f(x, y)\rightsquigarrow f(0, 0)$ 定义的映射R$[x, y]\longrightarrow$R.

(b) 由 $f(x)\rightsquigarrow f(2+\mathrm{i})$ 定义的映射R$[x]\longrightarrow$C.

9. 描述由 $f(x)\rightsquigarrow f(1+\sqrt{2})$ 定义的映射Z$[x]\longrightarrow$R 的核.

10. 描述由 $\varphi(x)=t$，$\varphi(y)=t^2$，$\varphi(z)=t^3$ 定义的同态 φ：C$[x, y, z]\longrightarrow$C$[t]$的核.

11. (a) 证明由 $x\rightsquigarrow t^2$，$y\rightsquigarrow t^3$ 定义的同态 φ:C$[x, y]\longrightarrow$C$[t]$的核是由多项式 y^2-x^3 生成的主理想.

(b) 具体确定 φ 的象.

12. 证明同态(3.8)的存在性.

13. 用任意有限域代替R 叙述并证明类似(3.8)的结果.

14. 证明如果两个环 R，R' 同构，那么多项式环 $R[x]$ 与 $R'[x]$ 也同构.

15. 设 R 是一个环，并设 $f(y)\in R[y]$ 是系数属于 R 的单变量多项式. 证明由 $x\rightsquigarrow x+f(y)$，$y\rightsquigarrow y$ 定义的映射 $R[x, y]\longrightarrow R[x, y]$ 是 $R[x, y]$ 的一个自同构.

16. 证明多项式 $f(x)=\sum a_ix^i$ 可以对 $x-a$ 的幂展开：$f(x)=\sum c_i(x-a)^i$，其中系数 c_i 是系数 a_i 的整系数多项式.

17. 设 R，R' 是环，而 $R\times R'$ 是它们的积. 确定下列映射中哪些是环同态.

(a) $R\longrightarrow R\times R'$，$r\rightsquigarrow(r, 0)$

(b) $R\longrightarrow R\times R$，$r\rightsquigarrow(r, r)$

(c) $R\times R'\longrightarrow R$，$(r_1, r_2)\rightsquigarrow r_1$

(d) $R\times R\longrightarrow R$，$(r_1, r_2)\rightsquigarrow r_1r_2$

(e) $R\times R\longrightarrow R$，$(r_1, r_2)\rightsquigarrow r_1+r_2$

18. (a) $\mathbb{Z}/(10)$是否与$\mathbb{Z}/(2)\times\mathbb{Z}/(5)$同构？

(b) $\mathbb{Z}/(8)$是否与$\mathbb{Z}/(2)\times\mathbb{Z}/(4)$同构？

19. 设 R 是特征为 p 的环. 证明由 $x\rightsquigarrow x^p$ 定义的映射 $R\longrightarrow R$ 是一个环同态. 这个映射称为*弗罗贝尼乌斯同态*.

20. 确定环$\mathbb{Z}[x]$的所有自同构.

21. 证明映射$\mathbb{Z}\longrightarrow R$(3.9)与正整数的乘法相容.

22. 证明域的特征是零或者素数.

23. 设 R 是特征为 p 的环. 证明如果 a 是幂零的，则 $1+a$ 是*幂单的*，即 $1+a$ 的某个幂等于 1.

24. (a) 环 R 的*诣零根* N 是其幂零元素的集合. 证明 N 是理想.

(b) 确定环$\mathbb{Z}/(12)$，$\mathbb{Z}/(n)$和$\mathbb{Z}$的诣零根.

25. (a) 证明推论(3.20).

(b) 证明推论(3.22).

26. 确定实系数形式幂级数环$\mathbb{R}[[t]]$的所有理想.

27. 在两个变量的多项式环 $F[x, y]$中找一个不是主理想的理想.

*28. 设 R 是环，并设 I 是多项式环 $R[x]$的理想. 假设 I 中非零元素的最低次数为 n 并且 I 中包含一个 n 次首一多项式. 证明 I 是一个主理想.

29. 设 I，J 是环 R 的理想. 举例说明 $I\cup J$ 不必是一个理想，但证明 $I+J=\{r\in R \mid r=x+y,\ x\in I,\ y\in J\}$是一个理想. 这个理想称为理想 I，J 的*和*.

30. (a) 设 I，J 是环 R 的理想. 证明 $I\cap J$ 是一个理想.

(b) 举例说明乘积的集合$\{xy \mid x\in I,\ y\in J\}$不必是一个理想，但 I 和 J 的元素乘积的有限和$\sum x_\nu y_\nu$ 的集合是一个理想. 这个理想称为*积理想*.

(c) 证明 $IJ\subset I\cap J$.

(d) 举例说明 IJ 与 $I\cap J$ 不必相等.

31. 设 I，J，J'是环 R 的理想. $I(J+J')=IJ+IJ'$是否成立？

*32. 如果 R 是非交换环，一个*理想*的定义是一个在加法下封闭的集合 I，使得如果 $r\in R$ 且 $x\in I$，则 rx 及 xr 都属于 I. 证明 $n\times n$ 实矩阵非交换环没有真理想.

33. 证明或推翻：如果对一个环 R 中的所有 a 都有 $a^2=a$，则 R 的特征为 2.

34. 环 S 的一个元素 e 称为*幂等的*，如果 $e^2=e$. 注意在环的积 $R\times R'$中，元素 $e=(1, 0)$是幂等的. 这个练习的目标是证明它的一个逆.

(a) 证明如果 e 是幂等元，则 $e'=1-e$ 也是幂等元.

(b) 设 e 是环 S 的一个幂等元. 证明主理想 eS 是一个环，其单位元为 e. 它可能不是 S 的子环，因为除非 $e=1$，否则它不包含 1.

(c) 设 e 是幂等元，并设 $e'=1-e$. 证明 S 同构于积环$(eS)\times(e'S)$.

第四节 商环与环的关系

1. 证明命题(4.9)的同态 φ 的象是命题中描述的子环.

2. 确定环$\mathbb{Z}[x]/(x^2+3, p)$的结构，其中(a) $p=3$，(b) $p=5$.

3. 描述下面每一个环.

381

(a) $\mathbb{Z}[x]/(x^2-3,2x+4)$ (b) $\mathbb{Z}[i]/(2+i)$

4. 证明命题(4.2).
5. 设 R' 由在环 R 引入关系 $\alpha=0$ 得到，并设 ψ: $R\longrightarrow R'$ 为典范映射. 证明这一构造的如下的泛性质：如果 $\varphi:R\longrightarrow\widetilde{R}$ 为一个环同态，且假设在 $\widetilde{R}$ 中 $\varphi(\alpha)=0$. 则存在唯一同态 φ': $R'\longrightarrow\widetilde{R}$ 使得 $\varphi'\circ\psi=\varphi$.
6. 设 I, J 是环 R 的理想. 证明 $I\cap J$ 的元素在 R/IJ 中的剩余是幂零的.
7. 设 I, J 是环 R 的理想，满足 $I+J=R$.

382

(a) 证明 $IJ=I\cap J$.

*(b) 证明中国剩余定理：对 R 的任一对元素 a, b, 存在一个元素 x 使得 $x\equiv a$(模 I)而 $x\equiv b$(模 J). [记号 $x\equiv a$(模 I)意为 $x-a\in I$.]

8. 设 I, J 是环 R 的理想，满足 $I+J=R$ 及 $IJ=0$.

(a) 证明 R 与积$(R/I)\times(R/J)$同构.

(b) 描述对应于这个积分解的幂等元(见第三节练习 34).

第五节 元素的添加

1. 描述由$\mathbb{Z}$添加一个满足关系 $2\alpha-6=0$ 及 $\alpha-10=0$ 的元素 α 所得到的环.
2. 假设在环$\mathbb{R}$ 添加一个满足关系 $\alpha^2=1$ 的元素 α. 证明得到的环同构于积环$\mathbb{R}\times\mathbb{R}$，并求$\mathbb{R}\times\mathbb{R}$ 中对应于 α 的元素.
3. 描述在积环$\mathbb{R}\times\mathbb{R}$ 中对元素(2, 0)取逆得到的环.
4. 证明元素 1, $t-\alpha$, $(t-\alpha)^2$, …, $(t-\alpha)^{n-1}$ 构成$\mathbb{C}[t]/((t-\alpha)^n)$的$\mathbb{C}$-基.
5. 用 α 表示 x 在环 $R'=\mathbb{Z}[x]/(x^4+x^3+x^2+x+1)$的剩余. 用基(1, α, α^2, α^3, α^4)计算表达式$(\alpha^3+\alpha^2+\alpha)(\alpha+1)$和 α^5.
6. 在下面每一情形，描述由在$\mathbb{F}_2$ 上添加满足给定关系的元素 α 所得到的环.

(a) $\alpha^2+\alpha+1=0$ (b) $\alpha^2+1=0$

7. 分析在$\mathbb{Z}$ 上添加满足一对关系 $\alpha^3+\alpha^2+1=0$ 和 $\alpha^2+\alpha=0$ 的一个元素 α 所得到的环.
8. 设 $a\in R$. 如果添加满足关系 $\alpha=a$ 的元素 α，我们期望又得到一个与 R 同构的环. 证明这是对的.
9. 描述在$\mathbb{Z}/12\mathbb{Z}$ 上添加 2 的逆所得到的环.
10. 确定在$\mathbb{Z}$ 上添加满足每一组关系的元素 α 得到的环 R'的结构.

(a) $2\alpha=6$, $6\alpha=15$ (b) $2\alpha=6$, $6\alpha=18$ (c) $2\alpha=6$, $6\alpha=8$

11. 设 $R=\mathbb{Z}/(10)$. 确定在环上添加满足每一关系的元素 α 得到的环的结构.

(a) $2\alpha-6=0$ (b) $2\alpha-5=0$

12. 设 a 是环 R 的单位. 描述环 $R'=R[x]/(ax-1)$.
13. (a) 证明如(5.9)所断言的，通过在多项式环 $R[x]$中对 x 取逆得到的环同构于洛朗多项式环.

(b) 形式洛朗级数 $\sum_{-\infty}^{\infty}a_nx^n$ 是否构成环?

14. 设 a 是环 R 的一个元素，且设 $R'=R[x]/(ax-1)$为由在 R 上添加 a 的逆得到的环. 证明映射 $R\longrightarrow R'$ 的核是使得对某个 $n>0$ 有 $a^nb=0$ 的元素 $b\in R$ 的集合.

383

15. 设 a 是环 R 的一个元素，且设 R'为由在 R 上添加 a 的逆得到的环. 证明 R'是零环当且仅当 a 是幂零元.
16. 设 F 是域. 证明环 $F[x]/(x^2)$与 $F[x]/(x^2-1)$同构当且仅当 F 的特征为 2.
17. 设 $\bar{R}=\mathbb{Z}[x]/(2x)$. 证明 $\bar{R}$ 的每一元素有唯一的形如 $a_0+a_1x+a_2x^2+\cdots+a_nx^n$ 的表达式，其中 a_i 为整数且 a_1, …, a_n 为 0 或 1.

第六节 整环与分式域

1. 证明整环的子环是整环.
2. 证明有限多个元素的整环是域.
3. 设 R 是整环. 证明多项式环 $R[x]$ 是整环.
4. 设 R 是整环. 证明多项式环 $R[x]$ 的可逆元素是 R 中的单位.
5. 是否存在恰好有 10 个元素的整环?
6. 证明域 F 上的形式幂级数环 $F[[x]]$ 的分式域由将单独一个元素 x 取逆得到, 将这个域的元素描述为具有负幂的幂级数.
7. 完成整环的分式等价类构成一个域的证明.
8. 半群 S 是具有满足结合律的合成法则且有单位元的集合. 设 S 是满足消去律的交换半群: $ab=ac$ 蕴涵 $b=c$. 用分式证明 S 可以嵌入一个群.
*9. 整环 R 的一个不包含零且在乘法下封闭的子集 S 称为一个*乘法集*. 给定一个乘法集 S, 定义 S-分式为形如 a/b 的元素, 其中 $b\in S$. 证明 S-分式的等价类构成一个环.

第七节 极大理想

1. 证明整数环的极大理想为由素数生成的主理想.
2. 确定下面每一个环的极大理想.

   (a) $\mathbb{R}\times\mathbb{R}$ (b) $\mathbb{R}[x]/(x^2)$ (c) $\mathbb{R}[x]/(x^2-3x+2)$ (d) $\mathbb{R}[x]/(x^2+x+1)$
3. 证明 $\mathbb{C}[x, y]$ 的理想 $(x+y^2, y+x^2+2xy^2+y^4)$ 是极大理想.
4. 设 R 是环, 并设 I 是 R 的一个理想. 设 M 是 R 包含 I 的理想, 并设 $\overline{M}=M/I$ 是 $\overline{R}$ 中对应的理想. 证明 M 是极大理想当且仅当 $\overline{M}$ 是极大理想.
5. 设 I 是 $\mathbb{C}[x, y]$ 中由多项式 y^2+x^3-17 生成的理想. 下列集合中那些在商环 $R=\mathbb{C}[x, y]/I$ 中生成极大理想?

   (a) $(x-1, y-4)$ (b) $(x+1, y+4)$ (c) (x^3-17, y^2)
6. 证明环 $\mathbb{F}_5[x]/(x^2+x+1)$ 是一个域.
7. 证明环 $\mathbb{F}_2[x]/(x^3+x+1)$ 是一个域, 但 $\mathbb{F}_3[x]/(x^3+x+1)$ 不是域.
8. 设 $R=\mathbb{C}[x_1, \cdots, x_n]/I$ 为 $\mathbb{C}$ 上多项式环的商, 并设 M 是 R 的极大理想. 证明 $R/M\approx\mathbb{C}$.
9. 定义 $\mathbb{R}[x]$ 的极大理想与上半平面的点的一一对应.
10. 设 R 是环, M 是 R 的一个理想. 假设 R 的每个不属于 M 的元素是 R 的单位. 证明 M 是极大理想而且它是 R 唯一的极大理想.
11. 设 P 是环 R 的理想. 证明 $\overline{R}=R/P$ 是整环当且仅当 $P\neq R$, 并且若 a, $b\in R$ 且 $ab\in P$, 则 $a\in P$ 或 $b\in P$. (满足这些条件的理想称为*素理想*.)
12. 设 $\varphi: R\longrightarrow R'$ 是环同态, 并设 P' 是 R' 的素理想.

    (a) 证明 $\varphi^{-1}(P')$ 是 R 的一个素理想.

    (b) 举出一个 P' 是极大理想但 $\varphi^{-1}(P')$ 不是极大理想的例子.
*13. 设 R 是分式域为 F 的整环, 并设 P 是 R 的素理想. 设 R_P 是 F 中由

$$R_P=\{a/d \mid a,d\in R, d\notin P\}$$

    定义的子集. 这个子集称为 R *在* P *处的局部化*.

    (a) 证明 R_P 是 F 的子环.

    (b) 确定 R_P 的所有极大理想.
14. 找一个"没有单位元素的环"的例子, 并求一个不含于极大理想的理想.

384

第八节　代数几何

1. 在下面的每一情形确定两个复平面曲线的交点.

(a) $y^2-x^3+x^2=1$，　$x+y=1$

(b) $x^2+xy+y^2=1$，　$x^2+2y^2=1$

(c) $y^2=x^3$，　$xy=1$

(d) $x+y+y^2=0$，　$x-y+y^2=0$

(e) $x+y^2=0$，　$y+x^2+2xy^2+y^4=0$

2. 证明除非两个二变量的二次多项式 f，g 有公共的非常数因式，否则它们最多有四个公共零点.

3. 由其经典型式(8.7)推导出希尔伯特零点定理.

4. 设 U，V 是$\mathbb{C}^n$ 的簇. 证明 $U\cup V$ 和 $U\cap V$ 都是簇.

5. 设 f_1，…，f_r；g_1，…，$g_s\in\mathbb{C}[x_1,\cdots,x_n]$，并设 U，V 分别是$\{f_1,\cdots,f_r\}$和$\{g_1,\cdots,g_s\}$的零点集. 证明如果 U 与 V 不相交，则$(f_1,\cdots,f_r;g_1,\cdots,g_s)$是单位理想.

6. 设 $f=f_1\cdots f_m$ 和 $g=g_1\cdots g_n$，其中 f_i，g_j 为$\mathbb{C}[x,y]$的既约多项式. 设 $S_i=\{f_i=0\}$及 $T_j=\{g_j=0\}$是由这些多项式定义的黎曼曲面. 并设 V 是簇 $f=g=0$. 用 S_i，T_j 描述 V.

7. 证明由一个多项式集合$\{f_1,\cdots,f_r\}$定义的簇仅与它们生成的理想$(f_1,\cdots,f_r)$有关.

8. 设 R 是一个环，包含$\mathbb{C}$为其子环.

(a) 说明如何将 R 变成$\mathbb{C}$的向量空间.

(b) 假设 R 是$\mathbb{C}$上的有限维向量空间，并设 R 恰好含有一个极大理想 M. 证明 M 是 R 的诣零根，即 M 恰好包含其所有幂零元.

385 9. 证明复圆锥曲线 $xy=1$ 同胚于删除一个点后的平面.

10. 证明$\mathbb{C}^2$ 的每一个簇是有限多个点和代数曲线的并.

11. 三个多项式 $f_1=x^2+y^2-1$，$f_2=x^2-y+1$ 和 $f_3=xy-1$ 生成$\mathbb{C}[x,y]$的单位理想. 用两种方法证明这个结论：(i)通过证明它们没有公共零点，(ii)通过将 1 写为 f_1，f_2，f_3 的具有多项式系数的线性组合.

12. (a) 确定代数曲线 S：$y^2=x^3-x^2$ 与直线 L：$y=\lambda x$ 的交点.

(b) 将 S 的点参数化为 λ 的函数.

(c) 用这个参数化将 S 与复 λ-平面联系起来.

*13. 理想 I 的根是 r 的某次幂属于 I 的元素 $r\in R$ 的集合.

(a) 证明理想 I 的根是一个理想.

(b) 证明由两个多项式集合$\{f_1,\cdots,f_r\}$和$\{g_1,\cdots,g_s\}$定义的簇相等当且仅当两个理想$(f_1,\cdots,f_r)$和$(g_1,\cdots,g_s)$有相同的根.

*14. 设 $R=\mathbb{C}[x_1,\cdots,x_n]/(f_1,\cdots,f_m)$. 设 A 是包含$\mathbb{C}$为子环的环. 求出下列集合间的一一对应：

(a) 在$\mathbb{C}$上为恒等映射的同态 $\varphi:R\longrightarrow A$.

(b) 方程组 $f_1=\cdots=f_m=0$ 的解，即对 $i=1,\cdots,m$ 有 $f_i(a)=0$ 的 A 的元素的 n-元组 $a=(a_1,\cdots,a_n)$.

杂题

1. 设 F 是域并设 K 表示向量空间 F^2. 由规则$(a_1,a_2)\cdot(b_1,b_2)=(a_1b_1-a_2b_2,a_1b_2+a_2b_1)$定义乘法.

(a) 证明这个法则与向量空间的加法使 K 成为一个环.

(b) 证明 K 是域当且仅当 F 中没有平方为-1的元素.

(c) 假设-1为 F 中的平方且 F 的特征不为 2，证明 K 同构于积环 $F\times F$.

2. (a) 可以对系数在环 R 中的任意多项式 $f(x)$用微分公式$(a_nx^n+\cdots+a_1x+a_0)'=na_nx^{n-1}+\cdots+1a_1$ 定义其导数. 利用同态(3.9)将整数系数解释为 R 中的元. 证明积公式$(fg)'=f'g+fg'$及链式法则$(f\circ g)'=$

$(f' \circ g)g'$.

(b) 设 $f(x)$ 是系数属于域 F 的多项式，并设 α 是 F 中的任一元素．证明 α 是 f 的一个重根当且仅当它是 f 及其导数 f' 的一个公共根．

(c) 设 $F=\mathbb{F}_5$．确定下列多项式在 F 中是否有重根：$x^{15}-x$，$x^{15}-2x^5+1$．

3. 设 R 是有两个合成法则的集合，满足除了加法交换律以外的所有的环的公理．通过用两种方式应用分配律展开积 $(a+b)(c+d)$ 来证明加法交换律．

4. 设 R 是一个环．确定多项式环中 $R[x]$ 的单位．

5. 设 R 表示最终为常数的实数序列的集合 $a=(a_1, a_2, a_3, \cdots)$：对充分大的 n 有 $a_n=a_{n+1}=\cdots$．加法和乘法按分量运算；即加法是向量加法而 $ab=(a_1b_1, a_2b_2, \cdots)$．

(a) 证明 R 是环．

(b) 确定 R 的极大理想．

6. (a) 对包含 $\mathbb{C}$ 且在 $\mathbb{C}$ 上向量空间的维数为 2 的环 R 分类．

*(b) 对 3 维作与(a)同样的分类．

386

*7. 考虑由 $f(x, y) \rightsquigarrow (f(x, 0), f(0, y), f(t, t))$ 定义的映射 $\varphi: \mathbb{C}[x, y] \longrightarrow \mathbb{C}[x] \times \mathbb{C}[y] \times \mathbb{C}[t]$．具体确定 φ 的象．

8. 设 S 是环 R 的子环．S 在 R 中的前导子 C 是使得 $\alpha R \subset S$ 的 R 的元素 $\alpha \in R$ 的集合．

(a) 证明 C 是 R 的一个理想也是 S 的一个理想．

(b) 证明 C 是 S 的同时也是 R 的理想的最大理想．

(c) 在下面三种情形中确定前导子：

(i) $R=\mathbb{C}[t]$，$S=\mathbb{C}[t^2, t^3]$；

(ii) $R=\mathbb{Z}[\zeta]$，$\zeta=\frac{1}{2}(-1+\sqrt{-3})$，$S=\mathbb{Z}[\sqrt{-3}]$；

(iii) $R=\mathbb{C}[t, t^{-1}]$，$S=\mathbb{C}[t]$．

9. $\mathbb{C}^2$ 的直线是线性方程 L：$\{ax+by+c=0\}$ 的轨迹．证明过两点 (x_0, y_0)，(x_1, y_1) 存在唯一一条直线，同时证明在给定的切方向 (u_0, v_0) 过一点 (x_0, y_0) 存在唯一一条直线．

10. $\mathbb{C}^2$ 的代数曲线 C 称为既约的，如果它是一个既约多项式 $f(x, y)$——不能分解为非常数多项式乘积的多项式——的零点的轨迹．点 $p \in C$ 称为曲线的奇点，如果在 p 点 $\partial f/\partial x=\partial f/\partial y=0$．否则 p 称为 C 的非奇点．证明既约曲线仅有有限多个奇点．

11. 设 L：$ax+by+c=0$ 是一条直线而 C：$\{f=0\}$ 是 $\mathbb{C}^2$ 的曲线．假设 $b \neq 0$．则可用直线的方程在 C 的方程 $f(x, y)$ 中消去 y，得到 x 的多项式 $g(x)$．证明其根是交点的 x-坐标．

12. 借助上一个问题的记号，L 与 C 在点 $p=(x_0, y_0)$ 的相交重数是 x_0 作为 g 的根的重数．直线称为 C 在 p 点的切线，如果相交重数至少为 2. 证明如果 p 是 C 的非奇点，则在 (x_0, y_0) 存在唯一一条切线，并计算该切线．

13. 证明如果 p 是曲线 C 的奇点，则每条直线过 p 点的相交重数至少为 2.

14. 既约曲线 C：$\{f=0\}$ 的次数 d 定义为既约多项式 f 的次数．

(a) 证明除非 $C=L$，否则 L 与 C 最多交于 d 个点．

*(b) 证明存在与 C 正好交于 d 个点的直线．

15. 求 $x^3+y^3-3xy=0$ 的奇点．

*16. 证明既约三次曲线最多有一个奇点．

*17. 曲线 C 上的一个非奇点 p 称为拐折点，如果 C 在 p 点的切线 L 与 C 在 p 点有一个至少为 3 的相交重数．

(a) 证明拐折点是 C 上黑塞矩阵

$$\det\begin{bmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x\,\partial y} & \frac{\partial f}{\partial x} \\ \frac{\partial^2 f}{\partial x\,\partial y} & \frac{\partial^2 f}{\partial y^2} & \frac{\partial f}{\partial y} \\ \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} & f \end{bmatrix}$$

为零的非奇点.

387 (b) 求三次曲线 y^2-x^3 与 $y^2-x^3+x^2$ 的拐折点.

*18. 设 C 是既约三次曲线，并设 L 是连接 C 上两个拐折点的直线. 证明如果 L 与 C 交于第三个点，则该点也是拐折点.

19. 设 $U=\{f_i(x_1,\cdots,x_m)=0\}$ 和 $V=\{g_j(y_1,\cdots,y_n)=0\}$ 是两个簇. 证明 $\mathbb{C}^{m+n}$ 中由 $\{f_i(x)=0,\ g_j(y)=0\}$ 定义的簇是积集 $U\times V$.

20. 证明 $\mathbb{R}^2$ 中轨迹 $y=\sin x$ 不位于任意代数曲线上.

*21. 设 f，g 是 $\mathbb{C}[x,y]$ 中的无公因式的多项式. 证明环 $R=\mathbb{C}[x,y]/(f,g)$ 是 $\mathbb{C}$ 上的有限维向量空间.

22. (a) 用 s，c 表示实直线上的函数 $\sin x$，$\cos x$. 证明它们生成的环 $\mathbb{R}[s,c]$ 是整环.

(b) 设 $K=\mathbb{R}(s,c)$ 表示 $\mathbb{R}[s,c]$ 的分式域. 证明域 K 同构于有理函数域 $\mathbb{R}(x)$.

*23. 设 $f(x)$，$g(x)$ 是系数在环 R 中的多项式且 $f\neq 0$. 证明如果积 $f(x)g(x)$ 为零，则存在一个非零元素 $c\in R$ 使得 $cg(x)=0$.

*24. 设 X 表示闭单位区间 $[0,1]$，R 是连续函数 $X\longrightarrow\mathbb{R}$ 的环.

(a) 证明在 X 中任一点都非零的函数 f 在 R 中可逆.

(b) 设 $f_1,\cdots,f_n$ 是在 X 上没有公共零点的函数. 证明这些函数生成的理想是单位理想.（提示：考虑 $f_1^2+\cdots+f_n^2$.）

(c) 建立 R 的极大理想与区间中的点的一一对应.

(d) 证明包含函数 f 的极大理想对应于区间中使 $f=0$ 的点.

(e) 将这些结果推广到 $\mathbb{R}^k$ 中的任意紧集 X 上.

388 (f) 描述 $X=\mathbb{R}$ 的情形.

第十一章 因子分解

唯真最美.

Hermann Minkowski

第一节 整数和多项式的因子分解

本章学习环中的除法. 由于它以整数环的性质为模型，我们将先复习这些性质. 其中一些在本书前几章就已不加说明地使用了，有些已经被证明.

由一个性质可以得出所有其他性质，这就是带余除法：若 a，b 是整数且 $a\neq 0$，则存在整数 q，r 使得

【1.1】
$$b = aq + r,$$
其中 $0\leqslant r<|a|$. 这个性质常只对正整数叙述，但它也允许 a，b 取负值. 这就是为什么要用绝对值 $|a|$ 来界定余数. (1.1)存在性的证明是一个简单的归纳证明.

回顾一下我们所看到的带余除法的一些最重要的结果. 在第十章，我们看到 $\mathbb{Z}^+$ 的每个子群是理想并且 $\mathbb{Z}$ 的每个理想是主理想，即存在整数 $d\geqslant 0$ 使之具有 $d\mathbb{Z}$ 的形式. 在第二章(2.6)已经证明，这蕴涵一对整数 a，b 的最大公因子存在并且它是 a 与 b 的一个整数线性组合. 如果 a 与 b 没有除 ± 1 以外的公因子，则 1 是 a 与 b 的整系数的线性组合：

【1.2】
$$ra + sb = 1,$$
对 r，$s\in\mathbb{Z}$ 成立. 这蕴涵第三章(2.8)所证明的素整数的基本性质. 在此复述如下：

389

【1.3】命题 *设 p 是素整数，并设 a，b 为任意整数. 如果 p 整除积 ab，则 p 整除 a 或 b.*

【1.4】定理 *算术基本定理：每个整数 $a\neq 0$ 可写为乘积*
$$a = cp_1\cdots p_k,$$
其中 $c=\pm 1$，p_i 是正素整数且 $k\geqslant 0$. 除了素因子的顺序外这个表达式是唯一的.

证明 首先，存在一个素分解. 为证明这一点，只需考虑 a 大于 1 的情形. 对 a 作归纳，可以假设存在性对所有正整数 $b<a$ 成立. 或者 a 是素数，这种情形下它是一个因数的积，或者它有一个真因数 $b\neq a$. 于是 $a=bb'$ 且也有 $b'\neq a$. b 和 b' 两个都比 a 小，由归纳假设它们可以分解成素数的乘积. 将它们的因子分解合起来就给出了 a 的因子分解.

其次分解是唯一的. 假设
$$\pm p_1\cdots p_n = a = \pm q_1\cdots q_m.$$
符号当然是一致的. 应用(1.3)，取 $p=p_1$. 由于 p_1 整除积 $q_1\cdots q_m$，它也整除某个 q_i，比如设为 q_1. 由于 q_1 是素数，$p_1=q_1$. 消去 p_1 并作归纳即可. ■

整数环的结构与域上一个变量的多项式环 $F[x]$ 的结构是非常类似的. 每当一个性质在这两个环之一上导出时，就应该在另一个环上找到相似的性质. 我们在第十章已经讨论了多项式的带余除法，并看到多项式环 $F[x]$ 的每个理想都是主理想[第十章(3.21)].

系数属于一个域 F 的多项式 $p(x)$ 称为既约的，如果它不是常数且它在 $F[x]$ 中仅有的低次数因子是常数. 这表明 p 可写为两个多项式乘积的方式仅有 $p=cp_1$，其中 c 是个常数而 p_1 是 p 的常数倍. 既约多项式与素整数类似. 按惯例通过消去其首项系数而对其正规化，使之成为首一多项式.

下面定理的证明与整数环类似的结论的证明相似：

【1.5】定理 设 F 是一个域，并设 $F[x]$ 表示 F 上的一元多项式环.

(a) 如果两个多项式 f, g 没有非常数的公因式，则存在多项式 r, $s\in F[x]$ 使得 $rf+sg=1$.

390

(b) 如果一个既约多项式 $p\in F[x]$ 整除乘积 fg，则 p 整除因子 f 或 g 之一.

(c) 每个非零多项式 $f\in F[x]$ 可以写成乘积

$$f = cp_1\cdots p_k,$$

其中 c 是非零常数，p_i 是 $F[x]$ 中首一的既约多项式，且 $k\geqslant 0$. 除了项的顺序外，这个因子分解是唯一的.

定理第三部分中出现的常数因子 c 类似于(1.4)中的因数 ± 1. 它们都是环的单位. 单位因子出现在这里是因为我们将素数都正规化为正的，而将既约多项式都正规化为首一的. 如果需要的话，也可允许有负素数及非首一的既约多项式. 如果 $k>0$，则单位因子可以被吸收掉. 但这将使唯一性的叙述变得有点复杂.

【1.6】例 在复数上，每一个正次数的多项式有一个根 α 因而有一个形如 $x-\alpha$ 的因式. 这样其既约多项式为线性的，且一个多项式的既约因式分解具有形式

【1.7】
$$f(x) = c(x-\alpha_1)\cdots(x-\alpha_n),$$

其中 α_i 是 $f(x)$ 的根，必要时可以是重复的. 这个因式分解的唯一性并不令人惊讶.

当 $F=\mathbb{R}$ 时，有两类既约多项式：线性多项式和二次既约多项式. 实二次多项式 x^2+bx+c 是既约的当且仅当其判别式 b^2-4c 是负的，这时它有一对共轭复根. 复数上每个既约多项式都是线性的这个事实蕴涵实数上没有更高次数的既约多项式. 假设多项式 $f(x)$ 的系数为实数 a_i 而 α 是 $f(x)$ 的一个的非实复根. 则复共轭 $\bar{\alpha}$ 不同于 α 因而也是一个根. 由于 f 是实多项式，其系数 a_i 满足关系 $a_i=\bar{a}_i$. 于是有

$$\begin{aligned} f(\bar{\alpha}) &= a_n\bar{\alpha}^n+\cdots+a_1\bar{\alpha}+a_0 \\ &= \bar{a}_n\bar{\alpha}^n+\cdots+\bar{a}_1\bar{\alpha}+\bar{a}_0 \\ &= \overline{f(\alpha)}=\bar{0}=0. \end{aligned}$$

二次多项式 $g(x)=(x-\alpha)(x-\bar{\alpha})=x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha}$ 有实系数 $-(\alpha+\bar{\alpha})$ 与 $\alpha\bar{\alpha}$，并且它的两个线性因式都出现在 $f(x)$ 的复因式分解(1.7)的右边. 这样 $g(x)$ 整除 $f(x)$. 因此 $f(x)$ 的实既约多项式的因式分解是由将其复因式分解中的共轭对集中起来得到的.

有理系数多项式的因式分解比实的和复的多项式的复杂得多，这是因为 $\mathbb{Q}[x]$ 中存在任意次数的既约多项式. 例如，x^5-3x^4+3 在 $\mathbb{Q}[x]$ 中是既约的. 在第四节中将看到更多的例子. 有理多项式的既约因式分解的形式和唯一性在直观上都是不清楚的.

391

我们注意下列的初等性质，以备将来之用：

【1.8】命题 设 F 是域，并设 $f(x)$ 是系数属于 F 的一个 n 次多项式. 则 f 在 F 中最多有 n 个根.

证明 一个元素 $\alpha\in F$ 是 f 的根当且仅当 $x-\alpha$ 整除 f[第十章(3.20)]. 这样，可记为 $f(x)=(x-\alpha)q(x)$，其中 $q(x)$ 是一个 $n-1$ 次的多项式. 如果 β 是 f 的另一个根，则 $f(\beta)=(\beta-\alpha)q(\beta)=0$. 由于 F 是域，F 中非零元素的乘积非零. 这样两个元素 $(\beta-\alpha)$，$q(\beta)$ 之一为零. 在第一种情形下 $\beta=\alpha$，而在第二种情形下 β 是 $q(x)$ 的一个根. 对 n 作归纳，可以假设 $q(x)$ 在 F 中最多有 $n-1$ 个根. 于是 β 最多有 n 种可能. ■

对于定理(1.5)和命题(1.8)，F 是一个域这个条件是关键的，如下面的例子所示. 设 R 是环 $\mathbb{Z}/8\mathbb{Z}$. 则在多项式环 $R[x]$ 中，有

$$x^2-1=(x+1)(x-1)=(x+3)(x-3).$$

多项式 x^2-1 模 8 有 4 个根，它因式分解为既约多项式的乘积不是唯一的.

第二节 唯一因子分解整环、主理想整环与欧几里得整环

看到多项式的因式分解与整数的因数分解类似，自然会问其他环是否也有这样的性质. 相对来说这样的环不多，但高斯整数环是一个有趣的例子. 本节探讨这一理论的各个部分可以拓广的方式.

首先引入用于研究因子分解的术语. 自然会假定所给的环 R 是整环，因而可以使用消去律，我们将始终要求有这个假定. 称一个元素 a 整除另一个元素 b(简写为 $a\mid b$)，如果存在 $q\in R$ 使得 $b=aq$. 元素 a 是 b 的*真因子*，如果存在 $q\in R$ 使得 $b=aq$ 并且 a 与 q 都不是单位. R 的非零元素 a 称为*既约的*，如果它不是单位且没有真因子. 两个元素 a，a' 称为*相伴的*，如果它们互相整除. 容易看出 a，a' 相伴当且仅当它们相差一个单位因子，即对某个单位 u 有 $a'=ua$.

因子、单位和相伴的概念可用由元素生成的主理想的语言来解释. 回忆理想 I 称为*主理想*，如果它由单独一个元素生成：

【2.1】
$$I=(a).$$

记住 (a) 是由 a 的所有倍元，即能被 a 整除的元素组成. 于是

392

【2.2】
$$\begin{aligned} u\text{ 是一个单位} &\Leftrightarrow (u)=(1)\\ a\text{ 和 }a'\text{ 相伴} &\Leftrightarrow (a)=(a')\\ a\text{ 整除 }b &\Leftrightarrow (a)\supset(b)\\ a\text{ 是 }b\text{ 的真因子} &\Leftrightarrow (1)>(a)>(b).\end{aligned}$$

这些等价的证明可直接得到，我们将其略去.

假设现在希望整环 R 中有一个类似于算术基本定理的定理. 我们可将定理的断言分成两部分. 第一，一个给定的元素 a 可以写成既约元的乘积；第二，这个积在实质上是唯一的.

考虑第一部分. 假设元素 a 不为零也不是单位；不然就没有把它写为既约元乘积的希望. 于是试图用下述过程分解 a：如果 a 本身是既约的，则已得到分解. 如果 a 不是既约的，则 a 有一个真因子，因而它以某种方式分解为乘积 $a=a_1b_1$，其中 a_1 或 b_1 都不是单位. 如果可能就继续分解 a_1 和 b_1，而且希望这一过程会停下来；换言之，希望在有限步后所有因子为既约

的．这一过程总是终止的条件用主理想有一个简洁的描述：

【2.3】命题 设 R 是整环．下列条件等价：

(a) 对 R 的每一个非单位的非零元 a，因子分解过程在有限多步后终止并将 a 因子分解成为 R 中既约元的乘积 $a=b_1\cdots b_k$.

(b) R 中不包含主理想的无限升链

$$(a_1)<(a_2)<(a_3)<\cdots.$$

证明 假设 R 中含有一个主理想的无限升链 $(a_1)<(a_2)<(a_3)<\cdots$. 则对所有 n 有 $(a_n)<(1)$，因为 $(a_n)<(a_{n+1})\subset(1)$. 由于 $(a_{n-1})<(a_n)$，a_n 是 a_{n-1} 的真因子，设 $a_{n-1}=a_nb_n$，其中 a_n，b_n 不是单位．这给出一个 a_1 的不会终止的因子分解序列：$a_1=a_2b_2=a_3b_3b_2=a_4b_4b_3b_2\cdots$. 反之，这样的一个因子分解序列给出一个理想的升链． ■

这个命题的第二个条件常称为主理想的升链条件．然而为了强调因子分解性质，如果命题中的等价条件成立，我们说在 R 中因子分解存在性成立．

容易描述因子分解存在性不成立的整环．一个例子是由在多项式环 $F[x_1]$ 上添加 x_1 的所有 2^k 次根得到的环：

393 **【2.4】**

$$R=F[x_1,x_2,x_3,\cdots],$$

满足关系 $x_2^2=x_1$，$x_3^2=x_2$，$x_4^2=x_3$，等等．在这个环中可以将元素 x_1 无限地分解，对应地存在一个主理想的无限升链 $(x_1)<(x_2)<(x_3)<\cdots$.

事实证明构造刚给出的例子需要无限多个环的生成元，因此我们很少会遇到这样的环．实际上，基本定理的第二部分是导致大部分麻烦的地方．因子分解为既约元通常是可能的，但它却不是唯一的．

环中的单位使得唯一性的叙述变得复杂．显然，单位因子应被忽略，因为成对添加 uu^{-1} 的可能性是无穷无尽的．出于同样的原因，相伴的因子应视为等价的．整数环中的单位是 ±1，在这个环中，我们自然地将其既约元(素数)正规化为正的；类似地，可以通过正规化既约多项式而坚持要求它们是首一的．在任意的整环中没有适当的方法来正规化其元素，因而允许某种程度的模糊．实际上使用主理想比使用元素更为简洁：相伴元生成同一个主理想．然而在这里使用元素并不太笨拙，我们仍将使用元素．理想的重要性在本章后面的几节里会变得清晰起来．

称一个整环 R 为唯一因子分解整环，如果它具有下面的性质：

【2.5】

(i) 因子分解的存在性对 R 成立．换言之，分解一个不是单位的非零元素 a 的过程在有限步后终止并得到一个因子分解 $a=p_1\cdots p_m$，其中每个 p_i 为既约的．

(ii) 一个元素的既约因子分解在下面的意义下是唯一的：如果 a 以两种方式分解为既约元，如设 $a=p_1\cdots p_m=q_1\cdots q_n$，则 $m=n$ 并且通过对因子适当地排序，对每个 i 有 p_i 与 q_i 相伴．

因而在唯一性的叙述中，相伴的因子分解被认为是等价的．

下面是一个因子分解的唯一性不成立的例子．环是整环

【2.6】
$$R=\mathbb{Z}[\sqrt{-5}].$$
它由所有形如$a+b\sqrt{-5}$的复数组成，其中a，$b\in\mathbb{Z}$．这个环的单位元是±1，且在R中整数6有两个本质上不同的因子分解：

【2.7】
$$6=2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5}).$$

不难证明所有四个项2，3，$1+\sqrt{-5}$，$1-\sqrt{-5}$都是R的既约元．由于单位是±1，2的相伴元是2和-2．所以2与$1\pm\sqrt{-5}$不相伴，这表明两个因子分解实质上是不同的，因此R不是唯一的因子分解整环．

394

素整数最关键的性质是：如果一个素数整除一个乘积，则它整除其因子中的一个．我们称整环R的一个元素p为*素的*，如果它具有下列性质：p不为零也不是单位，且如果p整除R中元素的乘积，则它整除其因子中的一个．正是这个性质导出了因子分解的唯一性．

【2.8】命题 *设R是一个整环．假设因子分解的存在性在R上成立．则R是唯一因子分解整环当且仅当每一个既约元都是素元．*

其证明是(1.3)和(1.4)论证的简单的拓广，我们将它留作练习．

重要的是区分既约元和素元这两个概念．在唯一因子分解整环中它们是相同的，但大多数环含有不是素元的既约元．例如，在上面所考虑的环$R=\mathbb{Z}[\sqrt{-5}]$中，元素2无真因子，因而它是既约的．然而它不是素元，因为虽然它整除$6=(1+\sqrt{-5})(1-\sqrt{-5})$，但它不整除其任一因子．

由于唯一因子分解整环中的既约元是素元，术语*既约因子分解*与*素因子分解*是同义词．在一个唯一因子分解整环中，可以交替使用它们，但在其他场合不行．

在一个唯一因子分解整环中有一个简单的方法，即用其既约因子分解或素因子分解来确定一个元素a是否整除另一个元素b．

【2.9】命题 *设R是一个唯一因子分解整环，并设$a=p_1\cdots p_r$，$b=q_1\cdots q_s$为R中给定的两个元素的素因子分解．则在R中a整除b当且仅当$s\geqslant r$，且适当排列b的因子q_i的顺序，对$i=1,\cdots,r$有p_i与q_i相伴．*

【2.10】推论 *设R是一个唯一因子分解整环，并设a，b是R中不全为零的两个元素．存在一个a，b的最大公因子d，它具有下列性质：*

(i) *d整除a和b；*

(ii) *如果R的一个元素e整除a和b，则e也整除d．*

由第二个性质，a，b的任意两个最大公因子是相伴的．然而最大公因子不一定具有$ra+sb$的形式．例如，在下一节将证明整多项式环$\mathbb{Z}[x]$是一个唯一因子分解整环[见(3.8)]．这个环中的元素2和x有最大公因子1，但1不是这两个元素的整多项式系数的线性组合．

395

整数环的另一个重要性质是$\mathbb{Z}$的每一个理想是主理想．每一个理想都是主理想的整环称为*主理想整环*．

【2.11】命题

(a) 在一个整环中，素元素是既约的．

(b) 在一个主理想整环中，既约元是素的.

我们将(2.9—2.11)的证明留作练习.

【2.12】**定理** 主理想整环是唯一因子分解整环.

证明 假设 R 是一个主理想整环. 则 R 的每个既约元都是素元. 因而由命题(2.8)，只需证明因子分解的存在性对 R 成立. 由命题(2.3)，这等价于证明 R 中没有主理想的无限升链. 用反证法. 假设$(a_1)<(a_2)<(a_3)<\cdots$是一个这样的链.

【2.13】**引理** 设 R 是任意环. 则一个理想的升链 $I_1\subset I_2\subset I_3\subset\cdots$的并是 R 的一个理想.

证明 设 I 表示升链的并. 如果 u，v 属于 I，则对某个 n 它们属于 I_n. 从而 $u+v$ 及 ru 亦属于 I_n；因此它们也属于 I. ■

将此引理应用于主理想链的并 I，并用 R 是主理想整环的假设得到 I 是主理想，设 $I=(b)$. 由于 b 属于理想(a_n)的并，它也属于其中一个理想. 但如果 $b\in(a_n)$，则$(b)\subset(a_n)$，而另一方面，$(a_n)\subset(a_{n+1})\subset(b)$，因而$(a_n)=(a_{n+1})=(b)$. 这与$(a_n)<(a_{n+1})$矛盾，这个矛盾完成了我们的证明.

定理(2.12)的逆不成立. 整多项式环$\mathbb{Z}[x]$是一个唯一因子分解整环[见(3.8)]，但它不是主理想整环.

【2.14】**命题**

(a) 设 p 是主理想整环 R 的非零元素，则 $R/(p)$是域当且仅当 p 是既约元.

(b) 极大理想是由既约元生成的主理想.

证明 由于一个理想 M 是极大的当且仅当 R/M 是域，因此两部分是等价的. 我们证明第二部分. 一个主理想(a)包含另一个主理想(b)当且仅当 a 整除 b. 一个既约元 p 仅有的因子是单位和 p 的相伴元. 因而包含(p)的主理想仅有(p)和(1). 由于 R 的每个理想是主理想，这表明一个既约元生成一个极大理想. 反之，设 b 是具有真因子分解 $b=aq$ 的元素，其中 a 及 q 都不是单位. 则$(b)<(a)<(1)$，这表明(b)不是极大的. ■

396

我们现在抽象带余除法过程. 为此，需要环的一个元素的大小的概念. 适当的度量有

【2.15】
$$\text{绝对值，如果}\quad R=\mathbb{Z}$$
$$\text{多项式的次数，如果}\quad R=F[x]$$
$$(\text{绝对值})^2\text{，如果}\quad R=\mathbb{Z}[\mathrm{i}]$$

一般来说，整环 R 上的大小函数是由 R 的非零元素的集合到非负整数的任意函数

【2.16】
$$\sigma: R-\{0\}\longrightarrow\{0,1,2,\cdots\}.$$

整环 R 是一个欧几里得整环，如果存在 R 上的一个大小函数σ使得除法算法成立：

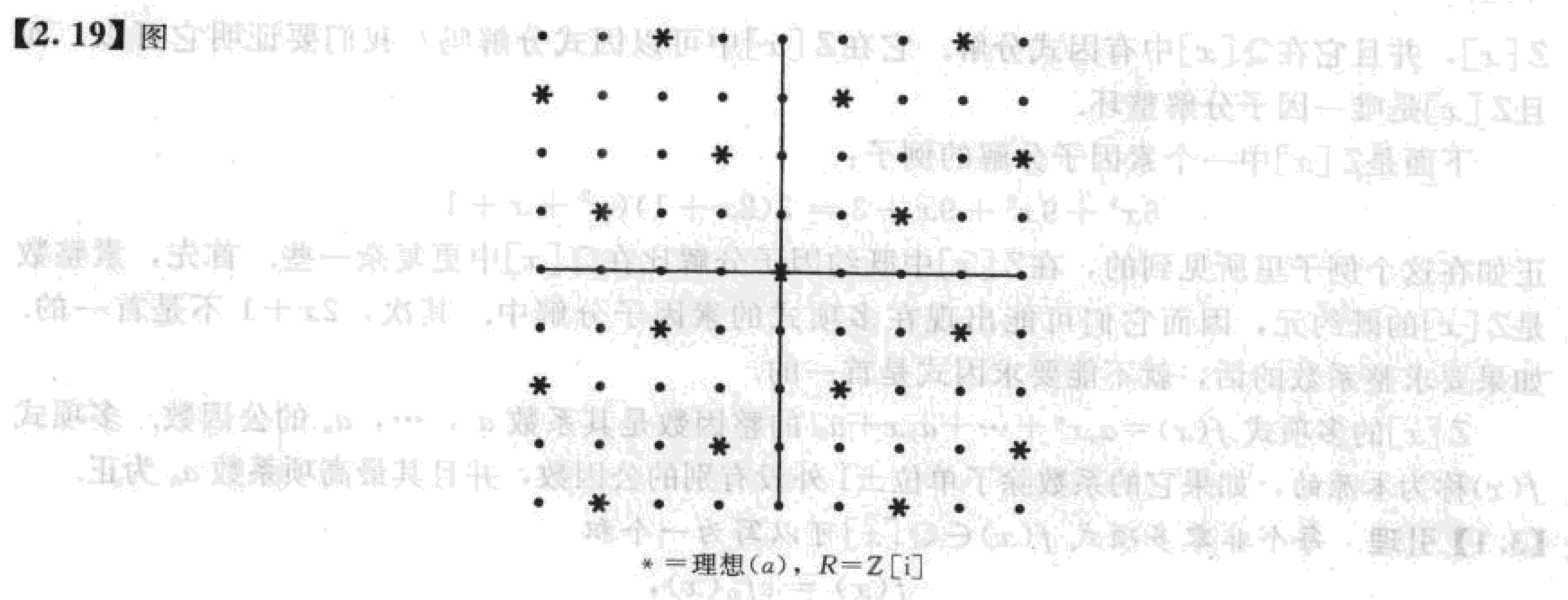
【2.17】设 a，$b\in R$ 并设 $a\neq0$. 则存在元素 q，$r\in R$ 使得 $b=aq+r$ 且 $r=0$ 或 $\sigma(r)<\sigma(a)$.

我们不要求元素 q，r 由 a，b 唯一确定.

【2.18】**命题** 环$\mathbb{Z}$，$F[x]$和$\mathbb{Z}[\mathrm{i}]$都是欧几里得整环.

整数环和多项式环已讨论过了. 我们证明高斯整数环是欧几里得整环，其大小函数为 $\sigma=|\ |^2$. $\mathbb{Z}[\mathrm{i}]$的元素构成复平面上的正方格，且一个给定元素 a 的倍数[也就是理想$(a)=Ra$]构成一个相似的格. 如果记 $a=re^{\mathrm{i}\theta}$，则(a)由转过角度 θ 然后用因子 $r=|a|$ 加以伸缩得到：

【2.19】图



$*$ = 理想(a)，$R=\mathbb{Z}[\mathrm{i}]$

397

显然，对于每个复数 b，至少存在格(a)中的一个点，它到 b 的距离的平方$\leqslant\frac{1}{2}|a|^2$. 设该点为 aq，并设 $r=b-aq$. 则 $|r|^2\leqslant\frac{1}{2}|a|^2<|a|^2$，这正是所要求的. 注意由于元素 aq 的选择可能不止一个，这个带余除法并不唯一.

也可以用代数方法进行证明. 用 a 除复数 b：$b=aw$，其中 $w=x+y\mathrm{i}$ 为复数，不必是高斯整数. 然后取离(x, y)最近的高斯整数点(m, n)，记 $x=m+x_0$，$y=n+y_0$，其中 m，n 是整数而 x_0，y_0 为实数且满足 $-\frac{1}{2}\leqslant x_0$，$y_0\leqslant\frac{1}{2}$. 则$(m+n\mathrm{i})a$ 为 Ra 中所求的点. 因为，$|x_0+y_0\mathrm{i}|^2<\frac{1}{2}$且$|b-(m+n\mathrm{i})a|^2=|a(x_0+y_0\mathrm{i})|^2<\frac{1}{2}|a|^2$.

可以复制整数因数分解的讨论并稍作变化以证明下面这个命题：

【2.20】命题 *欧几里得整环是主理想整环，因而是唯一因子分解整环.*

【2.21】推论 *环$\mathbb{Z}$，$\mathbb{Z}[\mathrm{i}]$和 $F[x]$(F 为域)是主理想整环和唯一因子分解整环.*

在高斯整数环$\mathbb{Z}[\mathrm{i}]$中 3 是既约的，因而是素的，但 2 和 5 不是既约的，因为

【2.22】
$$2=(1+\mathrm{i})(1-\mathrm{i}) \text{ 及 } 5=(2+\mathrm{i})(2-\mathrm{i})$$

这是 2 和 5 在$\mathbb{Z}[\mathrm{i}]$中的素因子分解.

在$\mathbb{Z}[\mathrm{i}]$中有四个单位，即$\{\pm1, \pm\mathrm{i}\}$. 于是环中每个非零元 α 有四个相伴元，即元素$\pm\alpha$，$\pm\mathrm{i}\alpha$. 例如 $2+\mathrm{i}$ 的相伴元为

$$2+\mathrm{i},\ -2-\mathrm{i},\ -1+2\mathrm{i},\ 1-2\mathrm{i}.$$

实际上，没有一个正规化$\mathbb{Z}[\mathrm{i}]$中素元的自然方法，虽然在有要求的时候可以选择位于第一象限且不在虚轴上的唯一的相伴元. 这里最好是接受(2.5)的多义性，要不然就使用主理想.

第三节 高斯引理

应用定理(1.5)到有理系数多项式环$\mathbb{Q}[x]$：每个多项式 $f(x)\in\mathbb{Q}[x]$可以唯一表示为 $cp_1\cdots p_k$ 的形式，其中 $c\in\mathbb{Q}$ 而 p_i 是$\mathbb{Q}$上既约的首一多项式. 现在假设多项式 $f(x)$有整系数，$f(x)\in$

$\mathbb{Z}[x]$，并且它在$\mathbb{Q}[x]$中有因式分解．它在$\mathbb{Z}[x]$中可以因式分解吗？我们要证明它可以，而且$\mathbb{Z}[x]$是唯一因子分解整环．

下面是$\mathbb{Z}[x]$中一个素因子分解的例子：

398

$$6x^3+9x^2+9x+3=3(2x+1)(x^2+x+1).$$

正如在这个例子里所见到的，在$\mathbb{Z}[x]$中既约因子分解比在$\mathbb{Q}[x]$中更复杂一些．首先，素整数是$\mathbb{Z}[x]$的既约元，因而它们可能出现在多项式的素因子分解中．其次，$2x+1$不是首一的．如果要求整系数的话，就不能要求因式是首一的．

$\mathbb{Z}[x]$的多项式$f(x)=a_nx^n+\cdots+a_1x+a_0$的整因数是其系数$a_0$，…，$a_n$的公因数．多项式$f(x)$称为本原的，如果它的系数除了单位$\pm1$外没有别的公因数，并且其最高项系数$a_n$为正．

【3.1】引理 每个非零多项式$f(x)\in\mathbb{Q}[x]$可以写为一个积

$$f(x)=cf_0(x),$$

其中c为有理数而$f_0(x)$是$\mathbb{Z}[x]$中的本原多项式．而且f的这个表达式是唯一的．多项式f是整系数的当且仅当c为整数．这时，$|c|$是f的系数的最大公因数，并且c的符号就是f的首项系数的符号．

引理中出现的有理数c称为$f(x)$的容量．如果f有整系数，则其容量在$\mathbb{Z}[x]$中整除f．而且，f是本原的当且仅当其容量为1．

引理的证明 要找到f_0，我们先用一个整数乘以f从而消去其系数的分母．这将给出一个整系数多项式f_1．然后分解出f_1的系数的最大公因数并调整其首项系数的符号．得到的多项式f_0是本原的，并且存在有理数c使得$f=cf_0$．这就证明了存在性．

要证唯一性，假设$cf_0(x)=dg_0(x)$，其中c，$d\in\mathbb{Q}$而f_0，g_0是本原多项式．我们要证明$c=d$和$f_0=g_0$．去掉分母则化为c和d都是整数的情形．设$\{a_i\}$，$\{b_i\}$分别表示f_0，g_0的系数．则对所有i有$ca_i=db_i$．由于$\{a_0,\cdots,a_n\}$的最大公因数是1，故c是$\{ca_0,\cdots,ca_n\}$的最大公因数．类似地，d是$\{db_0,\cdots,db_n\}=\{ca_0,\cdots,ca_n\}$的最大公因数．因此$c=\pm d$而$f_0=\pm g_0$．由于$f_0$和$g_0$的首项系数为正，$f_0=g_0$且$c=d$．如果$f$为整系数的，就不必去分母；因而$c$是整数，且在相差一个符号之下它是系数的最大公因数，这正是所断言的．■

如我们所看到的，代入原理给出一个同态

【3.2】
$$\mathbb{Z}[x]\longrightarrow\mathbb{F}_p[x],$$

其中$\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$是$p$元域．这个同态将多项式$f(x)=a_mx^m+\cdots+a_0$映到其模$p$剩余$\bar{f}(x)=\bar{a}_mx^m+\cdots+\bar{a}_0$．我们将用它来证明高斯引理．

399

【3.3】定理 高斯引理：$\mathbb{Z}[x]$中本原多项式的乘积是本原的．

证明 设多项式是f和g，它们的积是h．由于f和g的首项系数为正，因此h的首项系数也为正．要证h是本原的，只需证明不存在整除$h(x)$的所有系数的素整数p．这就证明了h的容量为1．考虑上面定义的同态$\mathbb{Z}[x]\longrightarrow\mathbb{F}_p[x]$．必须证明$\bar{h}\neq0$．由于$f$是本原的，它的系数不都能被$p$整除．因而$\bar{f}\neq0$．同样$\bar{g}\neq0$．由于多项式环$\mathbb{F}_p[x]$为整环，故$\bar{h}=\bar{f}\bar{g}\neq0$，这正是要证明的．■

【3.4】命题

(a) 设f，g是$\mathbb{Q}[x]$中的多项式，并设f_0，g_0是其在$\mathbb{Z}[x]$中相伴的本原多项式．如果在

$\mathbb{Q}[x]$中f整除g，则在$\mathbb{Z}[x]$中f_0整除g_0.

(b) 设f是$\mathbb{Z}[x]$中的本原多项式，设g是任意整系数多项式. 假设在$\mathbb{Q}[x]$中f整除g，比如存在$q\in\mathbb{Q}[x]$使得$g=fq$. 则$q\in\mathbb{Z}[x]$，因此f在$\mathbb{Z}[x]$中整除g.

(c) 设f，g是$\mathbb{Z}[x]$中的多项式. 如果它们在$\mathbb{Q}[x]$中有非常数公因式，则它们在$\mathbb{Z}[x]$中也有非常数公因式.

证明 要证(a)，我们可以去分母并使f和g变为本原多项式. 则(a)是(b)的结果. 要证(b)，我们应用(3.1)将商写为$q=cq_0$的形式，其中q_0是本原的而$c\in\mathbb{Q}$. 由高斯引理，fq_0是本原的，而等式$g=cfq_0$表明它是与g相伴的本原多项式g_0. 因而$g=cg_0$是引理(3.1)提到的g的表达式，而c是g的容量. 由$g\in\mathbb{Z}[x]$得到$c\in\mathbb{Z}$，因此$q\in\mathbb{Z}[x]$. 最后，为证明(c)，假定f，g在$\mathbb{Q}[x]$中有公因式h. 可设h是本原的，则由(b)，h在$\mathbb{Z}[x]$中同时整除f和g. ■

【3.5】推论 如果非常数多项式f在$\mathbb{Z}[x]$中是既约的，则它在$\mathbb{Q}[x]$中也是既约的.

【3.6】命题 设f是个具有正首项系数的整多项式. 则f在$\mathbb{Z}[x]$中是既约的当且仅当下列两条之一成立：

(i) f是素整数，或

(ii) f是本原多项式并且在$\mathbb{Q}[x]$中是既约的.

证明 假设f是既约的. 如引理(3.1)一样，可记$f=cf_0$，其中f_0是本原的. 由于f是既约的，它不会是一个真的因式分解. 因而c或f_0为1. 如果f_0为1，则f是常数，而一个常数多项式要为既约的，它必须是素数. 如果$c=1$，则f是本原的，由前面的推论可知它在$\mathbb{Q}[x]$中是既约的. 反之，整素数和本原既约多项式是$\mathbb{Z}[x]$中的既约元，这是显然的. ■ [400]

【3.7】命题 $\mathbb{Z}[x]$中的每一个既约元都是素元素.

证明 设f是既约的，并设f整除gh，其中g，$h\in\mathbb{Z}[x]$.

情形1：$f=p$是素整数. 如在(3.1)中一样，记$g=cg_0$而$h=dh_0$. 则g_0h_0是本原的，因此g_0h_0的某个系数a不为p整除. 但由于p整除gh，p也整除对应的系数，也就是cda. 因而p整除c或d，从而p整除g或h.

情形2：f是在$\mathbb{Q}[x]$中既约的本原多项式. 由(2.11b)，f是$\mathbb{Q}[x]$中的素元. 因此在$\mathbb{Q}[x]$中f整除g或h. 由(3.4)，f在$\mathbb{Z}[x]$中f也整除g或h. ■

【3.8】定理 多项式环$\mathbb{Z}[x]$是唯一因子分解整环. 每个不是± 1的非零多项式$f(x)\in\mathbb{Z}[x]$可以写为积

$$f(x)=\pm p_1\cdots p_m q_1(x)\cdots q_n(x),$$

其中p_i是素整数而$q_i(x)$为既约本原多项式. 这个表达式在因子重排后是唯一的

$\mathbb{Z}[x]$中因子分解的存在性是容易证明的，因而这个定理由命题(3.7)和(2.8)得到.

现设R是任意唯一因子分解整环，并设F是R的分式域[第十章(6.5)]. 则$R[x]$是$F[x]$的子环，并且如果所有的$\mathbb{Z}$用R代替而$\mathbb{Q}$用F代替，本节的结论皆可复制过去. 仅需要做的改动是，如上一节所述，最好用允许用有单位因子的多义性的本原多项式来代替正规化的本原多项式. 主要的结果如下：

【3.9】定理 设R是分式域为F的唯一因子分解整环.

(a) 设 f，g 是 $F[x]$ 中的多项式，并设 f_0，g_0 是它们在 $R[x]$ 中相伴的本原多项式．如果在 $F[x]$ 中 f 整除 g，则在 $R[x]$ 中 f_0 整除 g_0．

(b) 设 f 是 $R[x]$ 中的本原多项式，设 g 是 $R[x]$ 中任意的多项式．假设在 $F[x]$ 中 f 整除 g，比如存在 $q\in F[x]$ 使得 $g=fq$，则 $q\in R[x]$，因此 f 在 $R[x]$ 中整除 g．

(c) 设 f，g 是 $R[x]$ 中的多项式．如果它们在 $F[x]$ 中有非常数公因式，则它们在 $R[x]$ 中也有非常数公因式．

(d) 如果非常数多项式 f 在 $R[x]$ 中是既约的，则它在 $F[x]$ 中也是既约的．

(e) $R[x]$ 是唯一因子分解整环．

定理(3.9)的证明按照对环 $\mathbb{Z}[x]$ 建立起来的方式进行，我们将它略去．

由于 $R[x_1,\cdots,x_n]\approx R[x_1,\cdots,x_{n-1}][x_n]$，我们得到下面这个推论：

401 **【3.10】推论** 多项式环 $\mathbb{Z}[x_1,\cdots,x_n]$ 和 $F[x_1,\cdots,x_n]$ 是唯一因子分解整环，其中 F 是域．

因而两个变量的复多项式环 $\mathbb{C}[x,y]$ 是唯一因子分解整环．然而与单变量形成对比的是，单变量复多项式是线性多项式的积，而两个变量的多项式经常是既约的，因而也是素的．

多项式 $f(x,y)$ 的既约性有时可以通过研究 $\mathbb{C}^2$ 中的轨迹 $W=\{f(x,y)=0\}$ 来证明．假设 f 因式分解为

$$f(x,y)=g(x,y)h(x,y),$$

其中 g，h 是非常数多项式．则 $f(x,y)=0$ 当且仅当两个等式 $g(x,y)=0$ 或 $h(x,y)=0$ 之一成立．因而如果令 $U=\{g(x,y)=0\}$，$V=\{h(x,y)=0\}$ 表示 $\mathbb{C}^2$ 中的这两个簇，则

$$W=U\cup V.$$

有可能从几何上看出 W 有没有这样的分解．

例如，可以用这个方法证明多项式

$$f(x,y)=x^2+y^2-1$$

是既约的．因为 f 的总次数为 2，其真因子必是线性的，具有 $g(x,y)=ax+by+c$ 的形式．线性方程的解在一条直线上，而 $\{f=0\}$ 是圆．当然在提到直线和圆时，实际上说的是 $\mathbb{R}^2$ 中的实轨迹．因此这表明 f 在 $\mathbb{R}[x,y]$ 中是既约的．但事实上，圆的实轨迹上有足够多的点来证明它在 $\mathbb{C}[x,y]$ 中也是既约的．假设 $\mathbb{C}[x,y]$ 中 $f=gh$，其中 g 和 h 是如上所说的线性的．则实圆 $x^2+y^2-1=0$ 的每个点位于复轨迹 U，V 之一上．因而至少这两个轨迹之一有两个实点．恰好有一条复直线(一条直线是指线性方程 $ax+by+c=0$ 的解的轨迹)过两个给定的点，而这两个点是实的，于是定义直线的线性方程除了一个常数因子外也是实的．这通过具体写出过两点的直线方程就可证明．因而如果 f 有线性因子，则它有一个实的线性因子．但是圆中并不包含一条直线．

也可用待定系数法代数地证明 x^2+y^2-1 是既约的(见第四节练习 17)．

第四节　多项式的具体分解

现在提出确定一个给定的整多项式

【4.1】
$$f(x)=a_nx^n+\cdots+a_1x+a_0$$

的因式分解的问题．我们想要求的是 $\mathbb{Q}[x]$ 中的既约因式，由(3.5)这相当于确定 $\mathbb{Z}[x]$ 中的既

约因式. 其线性因子相当容易找到. 如果 b_1x+b_0 整除 $f(x)$, 则 b_1 整除 a_n 而 b_0 整除 a_0. 只存在有限多个整除 a_n 和 a_0 的整数, 于是可以尝试所有的可能情形. 在每一种情形我们做带余除法并确定其余式是否为零. 也可将有理数 $r=-b_0/b_1$ 代入 $f(x)$ 看它是否是一个根.

402

虽然对于高次因式不是那么清楚, 但克罗内克证明了因式都可通过有限步计算确定. 他的方法基于拉格朗日插值公式. 遗憾的是除了低次因式外, 这一方法所需要的步数太多而不实用, 因而在高效计算的问题上人们做了大量的工作. 一个最有用的方法之一是利用同态 $\mathbb{Z}[x]\longrightarrow\mathbb{F}_p[x]$ 的模 p 计算. 如果多项式 $f(x)$ 在 $\mathbb{Z}[x]$ 中有因式分解: $f=gh$, 则其模 p 剩余 $\bar{f}$ 也有因式分解 $\bar{f}=\bar{g}\bar{h}$. 而由于在 $\mathbb{F}_p[x]$ 中每一次数的多项式仅有有限多个, 所有因式分解可以在有限步内完成.

【4.2】命题 *设 $f(x)=a_nx^n+\cdots+a_0\in\mathbb{Z}[x]$ 是一个整多项式, 并设 p 是一个不整除 a_n 的素整数. 如果 f 模 p 的剩余 $\bar{f}$ 是既约的, 则 f 在 $\mathbb{Q}[x]$ 中是既约的.*

证明 这可通过检查同态得到. 我们需要假设 p 不整除 a_n 来排除 f 的因子 g 化为 $\mathbb{F}_p[x]$ 中常数的可能性. 当用与其相伴的本原多项式代替 f 时, 仍然保持这一假设. 因而可以假设 f 是本原的. 由于 p 不整除 a_n, 故 f 与 $\bar{f}$ 的次数相等. 如果 f 在 $\mathbb{Q}[x]$ 中可以进行因式分解, 则由推论(3.5), 它在 $\mathbb{Z}[x]$ 中也可进行因式分解. 设 $f=gh$ 是它在 $\mathbb{Z}[x]$ 中的真的因式分解. 由于 f 是本原的, g 与 h 有正次数. 由于 $\deg f=\deg\bar{f}$ 及 $\bar{f}=\bar{g}\bar{h}$, 于是得到 $\deg g=\deg\bar{g}$ 及 $\deg h=\deg\bar{h}$, 因此 $\bar{f}=\bar{g}\bar{h}$ 是真的因式分解, 这表明 $\bar{f}$ 可约. ■

假设怀疑一个给定的多项式 $f(x)\in\mathbb{Z}[x]$ 是既约的. 则可试着对一些小素数模 p 进行约比, 例如 $p=2, 3$, 这时希望 $\bar{f}$ 次数不变且是既约的. 如果是这样, 就证明了 f 也是既约的. 注意由于 $\mathbb{F}_p$ 是域, 对于环 $\mathbb{F}_p[x]$ 定理(1.5)的结论成立.

遗憾的是, 存在这样的整系数多项式, 虽然对所有素数 p 它们是模 p 可约的, 但其本身是既约的. 多项式 x^4-10x^2+1 是个例子. 因而模 p 约化的方法不总是可行的. 但它常常是有效的.

$\mathbb{F}_p[x]$ 中的既约多项式可用"筛法"找到. *埃拉托色尼筛法*是确定小于给定的数 n 的素数的方法. 列出从 2 到 n 的整数. 第一个 2 是素数, 因为 2 的真因数必小于 2, 而所列的数中没有比 2 小的数. 我们做一个记号标注 2 是素数这一事实, 然后在所列的数中划去 2 的倍数. 除去 2 本身以外, 它们都不是素数. 剩下的第一个数 3 是素数, 因为它不能被比它小的任何素数整除. 我们标注 3 是素数然后从所列的数中划去 3 的倍数. 剩下的下一个最小整数 5 也是个素数, 等等.

$$2\quad 3\quad \not{4}\quad 5\quad \not{6}\quad 7\quad \not{8}\quad \not{9}\quad \not{10}\quad 11\quad \not{12}\quad 13\quad \not{14}\quad \not{15}\quad \not{16}\quad 17\quad \not{18}\quad 19\quad \cdots$$

这一方法亦可确定 $\mathbb{F}_p[x]$ 的既约多项式. 我们按次数依次列出所有多项式, 然后划去乘积. 例如, $\mathbb{F}_2[x]$ 中的线性多项式为 x 及 $x+1$. 它们是既约的. 二次多项式为 x^2, x^2+x, x^2+1 及 x^2+x+1, 前面三个被 x 或 $x+1$ 整除, 因而最后一个是 $\mathbb{F}_2$ 上仅有的二次既约多项式.

403

【4.3】 $\mathbb{F}_2$ *上次数 $\leqslant 4$ 的既约多项式:*

$$x,\quad x+1;\quad x^2+x+1;\quad x^3+x^2+1,\quad x^3+x+1;$$
$$x^4+x^3+1,\quad x^4+x+1,\quad x^4+x^3+x^2+x+1.$$

用上面列出的多项式来试除, 我们可以在 $\mathbb{F}_2[x]$ 上分解所有 9 次以下的多项式.

作为(4.2)应用的一个例子，多项式 $x^4-6x^3+12x^2-3x+9$ 在 $\mathbb{Q}[x]$ 中是既约的，因为它在 $\mathbb{F}_2[x]$ 中的剩余是 x^4+x+1.

【4.4】 $\mathbb{F}_3$ 上的二次首一既约多项式：

$$x^2+1,\quad x^2+x-1,\quad x^2-x-1.$$

即使当模 p 的剩余可约时，它对刻画多项式的因式分解也是有帮助的. 作为例子，考虑多项式 $f(x)=x^3+6x+3$. 模 3 约化，我们得到 x^3. 这看起来起不了什么作用. 然而，假设 $f(x)$ 是可约的，比如设 $(ax+b)(cx^2+dx+e)=x^3+6x+3$. 则剩余 $ax+b$ 在 $\mathbb{F}_3[x]$ 中整除 x^3，这表明 $b\equiv 0$(模 3). 同样地，我们得到 $e\equiv 0$(模 3). 因为 $be=3$，这两个条件不可能同时得到满足. 因而没有这样的因式分解存在，从而 $f(x)$ 是既约的.

这个例子中起作用的原理称为艾森斯坦准则.

【4.5】命题 艾森斯坦准则：设 $f(x)=a_nx^n+\cdots+a_0\in\mathbb{Z}[x]$ 是一个整多项式，并设 p 是一个素整数. 假设 f 的系数满足下列条件：

(i) p 不能整除 a_n；

(ii) p 整除其余系数 $a_{n-1},\cdots,a_0$；

(iii) p^2 不能整除 a_0.

则 f 在 $\mathbb{Q}[x]$ 中是既约的. 如果 f 是本原的，则它在 $\mathbb{Z}[x]$ 中是既约的.

例如，$x^4+50x^2+30x+20$ 在 $\mathbb{Q}[x]$ 和 $\mathbb{Z}[x]$ 中是既约的.

艾森斯坦准则的证明 假设 f 满足条件. 设 $\bar{f}$ 表示模 p 的剩余. 假设(i)和(ii)表明 $\bar{f}=\bar{a}_nx^n$ 及 $\bar{a}_n\neq 0$. 如果 f 在 $\mathbb{Q}[x]$ 可约，它将在 $\mathbb{Z}[x]$ 中分解成正次数因子的积，如 $f=gh$. 则 $\bar{g}$ 和 $\bar{h}$ 整除 $\bar{a}_nx^n$，因此这两个多项式都是单项式. 因而 g 和 h 的所有系数(除去最高次系数)都被 p 整除. 设 g，h 的常系数为 b_0，c_0. 则 f 的常系数为 $a_0=b_0c_0$. 由于 p 整除 b_0 和 c_0，由此得 p^2 整除 a_0，这与(iii)矛盾. 这表明 f 是既约的. 最后一个断言由(3.6)得到. ■

404

艾森斯坦准则的最重要的应用之一是证明分圆多项式 $x^{p-1}+x^{p-2}+\cdots+x+1$ 的既约性，其根为 p 次单位根，即 $\zeta=e^{2\pi i/p}$ 的幂：

【4.6】推论 设 p 是素数. 多项式 $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ 在 $\mathbb{Q}[x]$ 中是既约的.

证明 我们注意到 $(x-1)f(x)=x^p-1$. 其次，用 $x=y+1$ 代入这个积，得到

$$yf(y+1)=(y+1)^p-1=y^p+\binom{p}{1}y^{p-1}+\binom{p}{2}y^{p-2}+\cdots+\binom{p}{p-1}y.$$

其中 $\binom{p}{i}=p(p-1)\cdots(p-i+1)/i!$. 如果 $i<p$，则素数 p 不是 $i!$ 的因数，因而 $i!$ 整除整数 $\binom{p}{i}$ 分子中剩下各项的乘积 $(p-1)\cdots(p-i+1)$. 这表明 $\binom{p}{i}$ 被 p 整除. 用 y 除 $yf(y+1)$ 的展开式表明 $f(y+1)$ 满足艾森斯坦准则的条件，因此它是一个既约多项式. 由此得到 $f(x)$ 也是既约的. ■

当用多项式环 $\mathbb{C}[t]$ 代替整数环时考察类似于艾森斯坦准则的断言是很有教益的. 这时用两个变量的多项式环 $\mathbb{C}[t][x]\approx\mathbb{C}[t,x]$ 代替了 $\mathbb{Z}[x]$.

【4.7】命题 设 $f(t,x)$ 是 $\mathbb{C}[t,x]$ 中的一个元素，写为以 t 的多项式为系数的 x 的多项式：

$f(t, x)=a_n(t)x^n+\cdots+a_1(t)x+a_0(t)$. 假设

(i) t 不整除 $a_n(t)$,

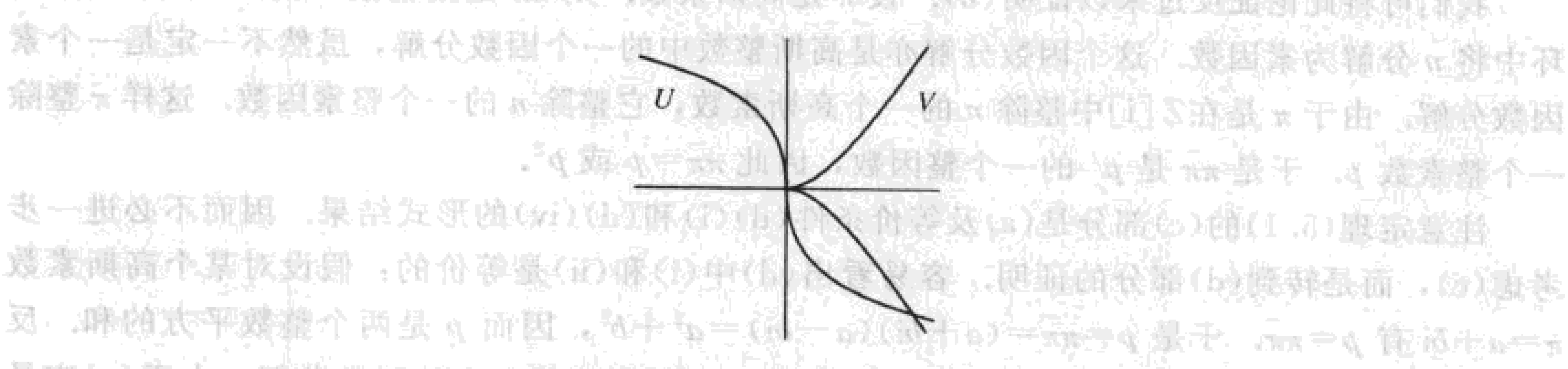
(ii) t 不整除 $a_{n-1}(t), \cdots, a_0(t)$,

(iii) t^2 不整除 $a_0(t)$.

则 $f(t, x)$在$\mathbb{C}(t)[x]$中是既约的. 如果 f 是本原的，就是说它没有只是 t 的多项式的因子，则 f 在$\mathbb{C}[t, x]$中是既约的.

这可以如(4.5)那样加以证明，用$\mathbb{C}[x]=\mathbb{C}[t, x]/(t)$替代$\mathbb{F}_p[x]$. 但通过考虑复 2-空间中的轨迹 $W=\{f(t, x)=0\}$来检查其几何性. (4.7)的条件(i)和(ii)蕴涵 $f(0, x)=cx^n$，其中 $c=a_n(0)\neq 0$. 结果在 $t=0$ 时 $f(t, x)=0$ 的解仅有 $t=x=0$，于是簇 W 仅与 x-轴$\{t=0\}$交于原点.

假设 $f(t, x)$是可约的：$f(t, x)=g(t, x)h(t, x)$. 于是 W 是两个簇 $U=\{g=0\}$及 $V=\{h=0\}$的并. 而且 $cx^n=f(0, x)=g(0, x)h(0, x)$. 因此 $g(0, x)$是 x^r 的一个常数倍，而 $h(0, x)$是 x^{n-r}的常数倍，其中 r 是 g 中变量 x 的次数. 因而 g 与 h 都在原点为零. 由此得到原点是 W 的奇点，也就是说偏导数$\partial f/\partial x$ 和$\partial f/\partial t$ 在(0, 0)都为零. 这可通过对积 gh 求导来检验. 另一方面，$\partial f/\partial t(0, 0)=\mathrm{d}a_0/\mathrm{d}t(0)$，而这是 $a_0(t)$的线性系数. 如果它为零，则 t^2 整除$a_0(t)$，与(4.7iii)矛盾. 405



第五节　高斯整数环中的素元

我们已看到高斯整数环是欧几里得整环. 其单位为$\{\pm 1, \pm \mathrm{i}\}$，并且每一个非零非单位元的元素是素元素的乘积. 本节将研究这些称为高斯素数的素元以及它们与素整数的关系. 我们在第二节里已看到了一些例子，这些例子中素数 5 在$\mathbb{Z}[\mathrm{i}]$中有因数分解：$5=(2+\mathrm{i})(2-\mathrm{i})$，而3 没有分解；3 是高斯素数. 记住由于有四个单位，故整数 5 有四个相伴的因式分解，我们认为它们是等价的：

$$(2+\mathrm{i})(2-\mathrm{i})=(-2-\mathrm{i})(-2+\mathrm{i})=(1-2\mathrm{i})(1+2\mathrm{i})=(-1+2\mathrm{i})(-1-2\mathrm{i}).$$

现在将证明例子 3 和例子 5 展示了在环$\mathbb{Z}[\mathrm{i}]$中素整数可以通过两种方式进行分解. 这可在下面的定理中加以总结：

【5.1】定理

(a) 设 p 是素整数. 则 p 或者是高斯素数，或者它是两个复共轭的高斯素数的乘积：$p=\pi\bar{\pi}$.

(b) 设 π 是高斯素数. 则 $\pi\bar{\pi}$ 或者是素整数，或者是素整数的平方.

(c) 作为高斯素数的素整数是模 4 与 3 同余的那些素整数，即 $p=3, 7, 11, 19, \cdots$.

(d) 设 p 是素整数. 下列结论等价:

(i) p 是两个复共轭高斯素数的乘积,

(ii) p 是两个整数的平方和: $p=a^2+b^2$, 其中 a, $b\in\mathbb{Z}$.

(iii) 同余式 $x^2\equiv-1$(模 p)有整数解.

(iv) $p\equiv1$(模 4)或 $p=2$; 即 $p=2, 5, 13, 17, \cdots$.

证明定理的所有部分得要花点时间.

406 由高斯整数的定义可直接得到下面的引理:

【5.2】引理 作为实数的高斯整数是通常的整数. 一个通常的整数 d 在 $\mathbb{Z}[i]$ 中整除另一个整数 a 当且仅当 d 在 $\mathbb{Z}$ 中整除 a. 而且, d 整除高斯整数 $a+bi$ 当且仅当 d 整除 a 和 b.

现在证明定理的(a)部分, 设 p 是一个整素数. 则 p 不是环 $\mathbb{Z}[i]$ 中的单位. 因此它有高斯素因数, 设其为 $\pi=a+bi$, 其中 a, $b\in\mathbb{Z}$. 因为 $\bar{p}=p$, 所以复共轭 $\bar{\pi}=a-bi$ 亦整除 p, 于是 $\pi\bar{\pi}=a^2+b^2$ 在高斯整数环中整除 p^2. 作为整数, $\pi\bar{\pi}$ 是 p^2 的整数因数有两种可能性: π 是 p 的一个相伴元. 这时 p 是一个高斯素数. 否则在高斯整数环中 π 是 p 的真因数, 这样在环 $\mathbb{Z}$ 中 $\pi\bar{\pi}$ 是 p^2 的真因数. 由于 $\pi\bar{\pi}$ 是正整数, 这时 $\pi\bar{\pi}=p$.

我们可将此论证反过来以证明(b). 设 π 是高斯素数. 则 $\pi\bar{\pi}$ 是正整数, 设 $\pi\bar{\pi}=n$. 在整数环中将 n 分解为素因数. 这个因数分解亦是高斯整数中的一个因数分解, 虽然不一定是一个素因数分解. 由于 π 是在 $\mathbb{Z}[i]$ 中整除 n 的一个高斯素数, 它整除 n 的一个整素因数. 这样 π 整除一个整素数 p. 于是 $\pi\bar{\pi}$ 是 p^2 的一个整因数, 因此 $\pi\bar{\pi}=p$ 或 p^2.

注意定理(5.1)的(c)部分是(a)及等价条件(d)(i)和(d)(iv)的形式结果. 因而不必进一步考虑(c), 而是转到(d)部分的证明. 容易看出(d)中(i)和(ii)是等价的: 假设对某个高斯素数 $\pi=a+bi$ 有 $p=\pi\bar{\pi}$. 于是 $p=\pi\bar{\pi}=(a+bi)(a-bi)=a^2+b^2$, 因而 p 是两个整数平方的和. 反之, 如果 $p=a^2+b^2$, 则 $p=(a+bi)(a-bi)$ 给出 p 在高斯整数环中的因数分解, 由于(a)它是一个素因数分解.

定理(5.1)的(d)(i)和(d)(iii)等价较难证明. 为此, 我们回到高斯整数的形式构造. 环 $\mathbb{Z}[i]$ 由在环 $\mathbb{Z}$ 上添加满足关系 $i^2+1=0$ 的元素 i 得到. 于是存在一个同构

【5.3】
$$\mathbb{Z}[x]/(x^2+1)\longrightarrow\mathbb{Z}[i].$$

设 (p) 是一个由素整数 p 在高斯整数环中生成的主理想. 其元素为 a 和 b 都被 p 整除的高斯整数 $a+bi$. 用 R' 记商环 $\mathbb{Z}[i]/(p)$. 则 R' 也可认为是通过在多项式环 $\mathbb{Z}[x]$ 上引入两个关系

【5.4】
$$x^2+1=0 \quad 及 \quad p=0$$

得到的环. 于是有一个同构

【5.5】
$$\mathbb{Z}[x]/(x^2+1,p)\longrightarrow\mathbb{Z}[i]/(p)=R',$$

其中 (x^2+1, p) 表示 $\mathbb{Z}[x]$ 中由两个元素生成的理想.

【5.6】引理 设 p 是素整数. 下列断言等价:

407 (i) p 是高斯素数;

(ii) 环 $R'=\mathbb{Z}[i]/(p)$ 是一个域;

(iii) x^2+1 是环 $\mathbb{F}_p[x]$ 的既约多项式.

证明　前两个断言的等价性由命题(2.14)得到. 我们真正要证的是(i)与(iii)等价，第一眼看上去，两个断言似乎是根本没有联系的. 就是为了得到这个等价关系我们才引入辅助的环R'. 证明基于下面这个初等但却特别有用的观察，它可由第三同构定理[第十章(4.3b)]得到：

【5.7】　为了构造环R',将(5.4)中的两个关系中的哪一个先引入环$\mathbb{Z}[x]$中都没有关系.

这样，我们反转其次序并从消去元素p开始. 代入原理告诉我们会得到什么. 同态$\mathbb{Z}[x]\longrightarrow\mathbb{F}_p[x]$的核正好就是理想$p\mathbb{Z}[x]$. 由于这个映射是满射，它导出同构

$$\mathbb{Z}[x]/p\mathbb{Z}[x]\xrightarrow{\sim}\mathbb{F}_p[x].$$

现在引入另一个关系x^2+1到这个环，将这个多项式的系数解释为$\mathbb{F}_p$的元素. 结果是一个同构

【5.8】
$$\mathbb{F}_p[x]/(x^2+1)\xrightarrow{\sim}R'.$$

把命题(2.14)应用到环$\mathbb{F}_p[x]$上就证明了R'是域当且仅当x^2+1在$\mathbb{F}[x]$中是既约的. ■

现在可以证明(5.1)的条件(d)(i)与(d)(iii)的等价性. 由引理(5.6)可知p是高斯素数当且仅当x^2+1在环$\mathbb{F}_p[x]$中是既约多项式. 由于它是二次多项式，x^2+1可约，如果它在$\mathbb{F}_p$中有一个根，而x^2+1不可约，如果它没有根. 而且整数a(模p)的剩余是x^2+1的根当且仅当$a^2\equiv-1$(模p). 这样，同余式$x^2\equiv-1$(模p)有解当且仅当x^2+1模p是可约的，它成立当且仅当p不是高斯素数. 这样便得到了(i)与(iii)等价.

剩下的是证明(d)中(iv)与其他条件等价. 我们将证明它与条件(iii)的等价. 同余式$x^2\equiv-1$(模2)的确有解$x=1$，因而只需看其他素数，即奇素数就行. 下一个引理解决了这个问题：

【5.9】引理　设p是奇素数并设$\bar{a}$表示整数a模p的剩余.

(a) 整数a是同余式$x^2\equiv-1$(模p)的解当且仅当其剩余$\bar{a}$是域$\mathbb{F}_p$的乘法群的一个4阶元素.

(b) 乘法群$\mathbb{F}_p^\times$含有一个4阶元素当且仅当$p\equiv1$(模4).

408

证明　$\mathbb{F}_p^\times$中恰好有一个2阶元素，即-1的剩余. 这是由于2阶元素是多项式x^2-1的一个根，并且我们知道这个多项式的根：它们在任意域中都是±1[见(1.7)]. 如果一个剩余$\bar{a}$在$\mathbb{F}_p^\times$中的阶为4，则$\bar{a}^2$的阶为2；因此$\bar{a}^2=-1$，这表明$a^2\equiv-1$(模p). 反之，如果$a^2\equiv-1$(模p)，则$\bar{a}$在$\mathbb{F}_p^\times$中的阶为4. 这证明了引理的(a).

现在群$\mathbb{F}_p^\times$的阶为$p-1$. 因而如果群包含一个4阶元素，则$p-1$被4整除，或等价地，$p\equiv1$(模4). 反之，假设$p-1$被4整除，并设H是$\mathbb{F}_p^\times$的西罗2-子群，其阶为整除$p-1$的2的最大的幂2^r. 由于4整除$p-1$，H的阶至少为4，因而在H中存在一个不同于±1的元素$\bar{a}$. 这个元素的阶不为2也不为1. 但由于H是2-群，$\bar{a}$的阶是2的幂. 从而$\bar{a}$的阶正好为4.

这就完成了定理(5.1)的证明. ■

第六节　代数整数

在下面几节将对一种简单而重要的情形，也就是二次虚整数的情形，讨论代数数的因数分解问题. 高斯整数环是这里的一个模型. 最初理想的引入正是为了将普通整数的因数分解的性质拓广到代数数，而这个拓广是非常漂亮的.

与我们所学的大多数主题不同，二次数域的算术并不具有普遍的重要性．它在算术中有许多应用，但在数学的其他领域里没有太多的应用．我们包括这一主题的原因，除了它的优美，就是它在历史上的重要性．我们的许多代数工具最初就是为了将整数的算术性质拓广到代数数而发展起来的．

代数数在算术上的一个典型应用是确定如

【6.1】 $$x^2+5y^2=p$$

的椭圆曲线的整点的问题，其中为了简单起见这里假设 p 是素数．为确定圆 $x^2+y^2=p$ 上的整点，可以分解左边得到 $(x+\mathrm{i}y)(x-\mathrm{i}y)=p$，然后用高斯整数的算术来分析其因数分解．在定理(5.1)的证明中就是这样做的．对方程(6.1)应用类似的方法得到

$$(x+\sqrt{-5}y)(x-\sqrt{-5}y)=p,$$

因而可设法在环 $\mathbb{Z}[\sqrt{-5}]$ 中进行分析．然而，正如我们所看到的，在这个环中因数分解不是唯一的．我们会有些麻烦．

另一个例子是著名的费马方程

409 【6.2】 $$x^3+y^3=z^3.$$

欧拉证明这个方程除了其中一个变量为零的平凡解以外没有整数解．为分析它，可将 y^3 移到另一边并作因式分解，得到

【6.3】 $$x^3=(z-y)(z-\zeta y)(z-\bar{\zeta}y),$$

其中

【6.4】 $$\zeta=\frac{1}{2}(-1+\sqrt{-3})=\mathrm{e}^{2\pi\mathrm{i}/3}$$

是1的复三次根．可以用环 $\mathbb{Z}[\zeta]$ 的算术分析这个方程．这个环是欧几里得整环，因而可以用唯一因数分解．遗憾的是(6.2)没有非平凡解的证明是相当复杂的，因而我们不会给出它的证明．

这一类求多项式方程的整数解的问题称为*丢番图问题*．我们要准备一些必要的工具，然后在第十二节讨论其中的几个．

一个复数 α 称为*代数的*，如果它是一个有理系数的非零多项式 $f(x)$ 的根(第十章第一节)．当然，可以消去多项式 $f(x)$ 系数的分母．因而如果 α 是一个代数数，则它也是整系数多项式的一个根．数 α 称为一个*代数整数*，如果它是一个首一的整系数多项式的根，即是形如

【6.5】 $$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0,\quad 其中\ a_i\in\mathbb{Z}$$

的多项式的根．这样作为多项式 x^3-1 的根，单位立方根 ζ 是一个代数整数．

设 α 是一个代数数．$\mathbb{Q}[x]$ 中以 α 为根的多项式全体的集合是由 $f(x)\rightsquigarrow f(\alpha)$ 定义的代入同胚

$$\mathbb{Q}[x]\longrightarrow\mathbb{C}$$

的核．因而它是一个主理想，由多项式环中的既约元 $f(x)$ 生成(为什么 f 是既约的)，这个多项式环称为 α *在* $\mathbb{Q}$ *上的既约多项式*．它是以 α 为根的次数最低的多项式并且在一个常数因子下是唯一的．α 的既约多项式的次数称为 α *在* $\mathbb{Q}$ *上的次数*．

可将 α 的这个既约多项式 $f(x)$ 取作 $\mathbb{Z}[x]$ 中的本原多项式．则 $f(x)$ 也生成 $\mathbb{Z}[x]$ 中所有以 α 为根的整系数多项式的理想．

【6.6】命题 使 $x \rightsquigarrow \alpha$ 的映射 $\mathbb{Z}[x] \longrightarrow \mathbb{C}$ 的核是由 α 的本原既约多项式生成的 $\mathbb{Z}[x]$ 的主理想.

证明 设 $f(x)$ 是 α 的本原既约多项式. 如果 $g \in \mathbb{Z}[x]$ 以 α 为根，则在 $\mathbb{Q}[x]$ 中 f 整除 g，因此由(3.4)在 $\mathbb{Z}[x]$ 中 f 也整除 g. 因而 g 属于 $\mathbb{Z}[x]$ 中由 f 生成的主理想. ■ 410

注意多项式 $f(x)$ 的首项系数整除其在 $\mathbb{Z}[x]$ 中任意倍数的首项系数. 因此由命题(6.6)，如果 α 的本原既约多项式 $f(x)$ 不是首一的，则 α 不是任意首一整多项式的根.

【6.7】命题 一个代数数 α 是代数整数当且仅当 α 的本原既约多项式是首一的. 等价地，α 是代数整数当且仅当 α 在 $\mathbb{Q}[x]$ 中的首一既约多项式是整系数的.

单位立方根 ζ 的本原既约多项式是 x^2+x+1.

【6.8】推论 一个有理数 r 是代数数当且仅当它是一个普通整数.

这是因为有理数 r 在 $\mathbb{Q}$ 上的首一既约多项式是 $x-r$.

命题(6.7)可用于确定一个代数数是否是代数整数，假如可以算出它的既约多项式的话. 例如，$\alpha=\frac{1}{2}(1+\sqrt{2})$ 是 $4x^2-4x-1$ 的根. 这是 α 的一个本原既约多项式. 因此 α 不是一个代数整数.

代数整数的概念是数论中最重要的发现之一. 不容易很快地解释为什么它是最为恰当的定义，但粗略地说，可以把 α 的本原既约多项式的首项系数 $f(x)$ 看作"分母". 如果 α 是一个整多项式 $f(x)=dx^n+a_{n-1}x^{n-1}+\cdots+a_0$ 的根，则 $d\alpha$ 是个代数整数，因为它是首一整多项式

【6.9】
$$x^n+a_{n-1}x^{n-1}+d\,a_{n-2}x^{n-2}+\cdots+d^{n-2}a_1x+d^{n-1}a_0$$

的一个根. 这样可以对任意代数数 α 通过乘上一个适当的整数"去分母"而得到一个代数整数. 然而，首项系数并不是一个精确的分母. 这样当 $\alpha=\frac{1}{2}(1+\sqrt{2})$ 时，2α 是个代数整数，而它的本原既约多项式的首项系数是 4.

另一方面，代数整数 $\zeta=\frac{1}{2}(-1+\sqrt{-3})$ 表明不能仅因为某些代数数的表达式有分母就仓促地作出它不是代数整数的结论.

代数整数的具体计算并不容易. 它们构成 $\mathbb{C}$ 的一个子环，即代数整数的和与积仍是代数整数，这是一个事实并不明显的事实. 我们不会去建立一般的理论，而只具体讨论二次扩张的情形.

二次数域 $F=\mathbb{Q}[\sqrt{d}]$ 由所有复数

【6.10】
$$a+b\sqrt{d},\quad a,b\in\mathbb{Q}$$

组成，其中 d 是一个固定的整数，正负皆可但不是有理数的平方. $\sqrt{d}$ 在 $d>0$ 时表示正平方根而在 $d<0$ 时表示正虚平方根. 如果 d 有整数平方因子，则可将其提到根号外并放入 b 中而不会改变域. 因而习惯上假设 d 是无平方的，也就是说 $d=\pm p_1\cdots p_r$，其中 p_i 是互不相同的素数，或 $d=-1$. 因而我们的取值为 411

$$d=-1,\pm2,\pm3,\pm5,\pm6,\pm7,\pm10,\cdots.$$

当 $d>0$ 时域 F 称为实二次数域，而当 $d<0$ 时称为虚二次数域.

现在计算 F 中的代数整数. 对特殊的 d 值的计算并不比一般情形简单. 然而，在做这一计算时可能会想要作一个如 $d=5$ 之类的代人. 令

【6.11】
$$\delta=\sqrt{d}.$$

410

当 d 为负时 δ 是纯虚数. 设

$$\alpha=a+b\delta$$

为 F 中不属于$\mathbb{Q}$的任意元素，即有 $b\neq 0$. 则 $\alpha'=a-b\delta$ 亦属于 F. 如果 d 为负，则 α'是 α 的复共轭. 注意 α 是多项式

【6.12】
$$(x-\alpha)(x-\alpha')=x^2-(\alpha+\alpha')x+\alpha\alpha'=x^2-2ax+(a^2-b^2d)$$

的一个根. 这个多项式的系数是有理数 $-2a$ 和 a^2-b^2d. 由于 α 不是有理数，故它不是线性多项式的根. 因而(6.12)是既约的，所以它是 α 在$\mathbb{Q}$上的首一既约多项式. 根据(6.7)，α 是代数整数当且仅当(6.12)是整系数的. 这样有下面的推论：

【6.13】推论 *$\alpha=a+b\delta$ 是代数整数当且仅当 $2a$ 和 a^2-b^2d 是整数.*

当 $b=0$ 时推论也成立，因为如果 a^2 是整数，则 a 也是. 如果愿意的话，可以用推论的条件作为 F 中整数的定义.

a 和 b 的可能取值依赖于 d 模 4 的同余类. 注意由于假定 d 是无平方的，$d\equiv 0$(模 4)的情形已被排除掉，因而 $d\equiv 1$，2 或 3(模 4).

【6.14】命题 *二次域 $F=\mathbb{Q}[\sqrt{d}]$ 的代数整数具有 $\alpha=a+b\delta$ 的形式，其中：*

(a) 如果 $d\equiv 2$ 或 3(模 4)，则 a 和 b 是整数.

(b) 如果 $d\equiv 1$(模 4)，则或者 a，$b\in\mathbb{Z}$ 或者 a，$b\in\mathbb{Z}+\frac{1}{2}$.

三次单位根 $\xi=\frac{1}{2}(-1+\sqrt{-3})$是一个第二类型的代数整数的例子. 另一方面，由于$-1\equiv$

412

3(模 4)，$\mathbb{Q}[i]$中的整数恰好是高斯整数.

命题的证明 由于 α 的既约多项式(6.12)的系数是 $2a$ 和 a^2-b^2d，如果 a，b 为整数，则 α 当然是代数整数. 假设 $d\equiv 1$(模 4)且 a，$b\in\mathbb{Z}+\frac{1}{2}$. (我们说它们是半整数.)于是 $2a\in\mathbb{Z}$. 要证 $a^2-b^2d\in\mathbb{Z}$，记 $a=\frac{1}{2}m$，$b=\frac{1}{2}n$，其中 m，n 为奇整数. 模 4 计算得

$$m^2-n^2d\equiv(\pm 1)^2-(\pm 1)^2\cdot 1\equiv 0(\text{模 }4).$$

因此 $a^2-b^2d=\frac{1}{4}(m^2-n^2d)\in\mathbb{Z}$，这正是要证的.

反之，假设 α 是代数整数. 则由推论(6.13)，$2a\in\mathbb{Z}$. 有两种情形：$a\in\mathbb{Z}$，或者 $a\in\mathbb{Z}+\frac{1}{2}$.

411

情形 1：$a\in\mathbb{Z}$. 由此亦得到 $b^2d\in\mathbb{Z}$. 如果记 $b=m/n$，其中 m，n 为互素整数且 $n>0$，则 $b^2d=m^2d/n^2$. 由于 d 是无平方的，它不能约去分母中的一个平方. 因此 $n=1$. 如果 a 是整数，则 b 也必是整数.

情形 2：$a\in\mathbb{Z}+\frac{1}{2}$是半整数，如前面一样，设 $a=\frac{1}{2}m$. 于是 $4a^2\in\mathbb{Z}$ 且条件 $a^2-b^2d\in\mathbb{Z}$

蕴涵 $4b^2d\in\mathbb{Z}$ 而 $b^2d\notin\mathbb{Z}$. 因而 b 也是半整数，设 $b=\frac{1}{2}n$，其中 n 是奇数. 要使这时 a，b 的值满足 $a^2-b^2d\in\mathbb{Z}$，必须有 $m^2-n^2d\equiv 0$(模 4). 模 4 计算得到 $d\equiv 1$(模 4). ■

在 $d\equiv 1$(模 4)的情形写出所有整数的一个方便的方法是引入代数整数

【6.15】
$$\eta=\frac{1}{2}(1+\delta),$$

它是首一整多项式

【6.16】
$$x^2-x+\frac{1}{4}(1-d)$$

的根.

【6.17】命题 假设 $d\equiv 1$(模 4). 则 $F=\mathbb{Q}[\sqrt{d}]$的代数整数为 $a+b\eta$，其中 a，$b\in\mathbb{Z}$.

容易通过具体计算证明，在每一种情形下 F 中的整数构成一个环 R，称为 F 中的**整数环**，用高中学过的代数可进行 R 中的计算.

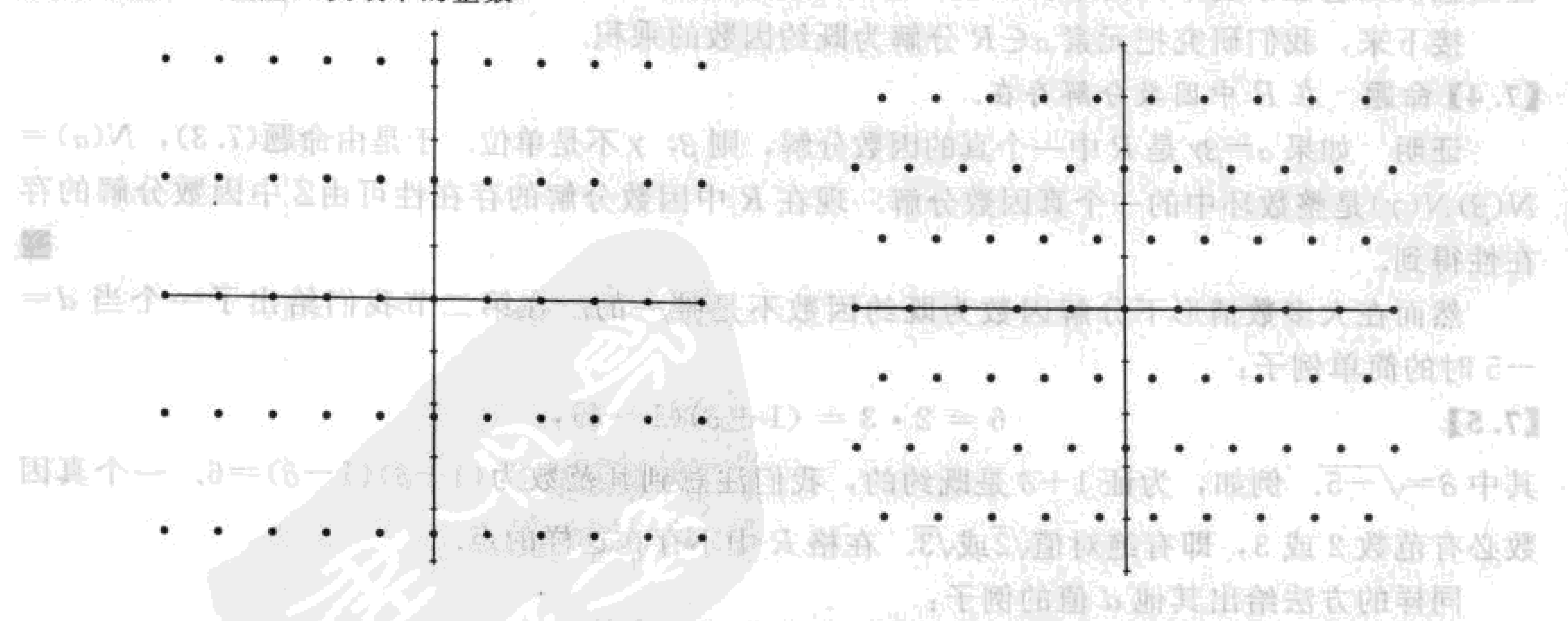
当 $R=\mathbb{Z}[\delta]$时 F 的**判别式**定义为多项式 x^2-d 的判别式，而在 $R=\mathbb{Z}[\eta]$时定义为多项式 $x^2-x+\frac{1}{4}(1-d)$的判别式. 这个判别式记为 D. 这样

【6.18】
$$D=\begin{cases}4d, & \text{如果 } d\equiv 2,3\\ d, & \text{如果 } d\equiv 1\end{cases}\ (\text{模 } 4).$$

由于 D 可用 d 算出，单独为它引入一个记号并不是非常重要的. 然而有些公式用 D 而不用 d 表出时会变得与共轭类无关.

虚二次域 $d<0$ 的情形处理起来比实的情形要容易些，我们将在下节专门加以讨论. 在虚的情形，环 R 形成复平面上的格，如果 $d\equiv 2$，3(模 4)，它是长方形的，而如果 $d\equiv 1$(模 4)，它是"等腰三角形". 当 $d=-1$ 时，R 是高斯整数环，格是正方形的. 当 $d=-3$ 时，格是等边三角形. 另外两个例子图示如下.

【6.19】图 一些虚二次域中的整数



成为格这一性质是这里所考虑的环所特有的，我们将用几何来分析它们. 把 R 作为格在直观上也是有用的.

在我们的讨论中考察一个特殊例子是有益的. 将 $d=-5$ 的情形取作此用. 由于 $-5\equiv 3$(模 4)，整数环形成一个长方形的格，且 $R=\mathbb{Z}[\delta]$，其中 $\delta=\sqrt{-5}$.

第七节　虚二次域中的因数分解

设 R 是一个虚二次数域 $F=\mathbb{Q}[\delta]$中的整数环. 如果 $\alpha=a+b\delta$ 属于 R，则其复共轭 $\bar{\alpha}=a-b\delta$ 也属于 R. 我们称整数

【7.1】
$$N(\alpha)=\alpha\bar{\alpha}$$
为 α 的范数. 它也等于 a^2-b^2d 和 $|\alpha|^2$，并且是 α 在 $\mathbb{Q}$ 上的既约多项式的常数项. 这样除非 $\alpha=0$，否则 $N(\alpha)$是正整数. 注意

414 【7.2】
$$N(\beta\gamma)=N(\beta)N(\gamma).$$
这个公式给出了对 R 中元素 α 的可能的因数的限制. 设 $\alpha=\beta\gamma$. 则(7.2)右边的两项皆为正整数. 因而要验证 α 的因数，只需找其范数整除 $N(\alpha)$的元素 β 就行了；当 a 和 b 都适当的小时这不是一个太大的工作.

特别地，我们求 R 的单位：

【7.3】命题

(a) R 的元素 α 是单位当且仅当 $N(\alpha)=1$.

(b) 除非 $d=-1$ 或 -3，否则 R 的单位都是$\{\pm 1\}$. 如果 $d=-1$，则 R 是高斯整数环，单位为$\{\pm 1, \pm i\}$，而如果 $d=-3$，则它们是 6 次单位根$\frac{1}{2}(1+\sqrt{-3})$的幂.

证明　如果 α 是单位，则 $N(\alpha)N(\alpha^{-1})=N(1)=1$. 由于 $N(\alpha)$和 $N(\alpha^{-1})$为正整数，它们都等于 1. 反之，如果 $N(\alpha)=\alpha\bar{\alpha}=1$，则$\bar{\alpha}=\alpha^{-1}$. 于是 $\alpha^{-1}\in R$，并且 α 是单位. 这样 α 是单位当且仅当它位于复平面的单位圆上. 第二个断言由格 R 的构造得到[见图(6.19)]. ■

接下来，我们研究把元素 $\alpha\in R$ 分解为既约因数的乘积.

【7.4】命题　在 R 中因数分解存在.

证明　如果 $\alpha=\beta\gamma$ 是 R 中一个真的因数分解，则 β，γ 不是单位. 于是由命题(7.3)，$N(\alpha)=N(\beta)N(\gamma)$是整数环中的一个真因数分解. 现在 R 中因数分解的存在性可由$\mathbb{Z}$中因数分解的存在性得到. ■

然而在大多数情形下分解因数为既约因数不是唯一的. 在第二节我们给出了一个当 $d=-5$ 时的简单例子：

【7.5】
$$6=2\cdot 3=(1+\delta)(1-\delta),$$
其中 $\delta=\sqrt{-5}$. 例如，为证 $1+\delta$ 是既约的，我们注意到其范数为$(1+\delta)(1-\delta)=6$. 一个真因数必有范数 2 或 3，即有绝对值$\sqrt{2}$或$\sqrt{3}$. 在格 R 中不存在这样的点.

同样的方法给出其他 d 值的例子：

【7.6】命题　满足 $d\equiv 3$(模 4)的唯一因子分解整环 R 只有高斯整数环.

证明 假设 $d\equiv 3$(模 4)，而 $d\neq -1$. 则

$$1-d=2\left(\frac{1-d}{2}\right),\quad 1-d=(1+\delta)(1-\delta).$$

在 R 中 $1-d$ 有两个因数分解. 因为 $N(2)=4$ 是 $N(\alpha)$ 所取的 >1 的最小值，所以元素 2 是既约的. [当 $d=-5,\ -13,\ -17,\ \cdots$ 时，在以原点为圆心 2 为半径的圆中 R 中仅有的点是 0，1，-1. 见图(6.19)]. 于是如果上述因数分解有一个公共的加细，则 2 在 R 中必整除 $1+\delta$ 或 $1-\delta$，这是不对的：当 $d\equiv 3$(模 4)时，$\frac{1}{2}\pm\frac{1}{2}\delta$ 不属于 R. ■

注意如果 $d\equiv 1$(模 4)，这个推理会失效. 在这种情形，由于 $\frac{1}{2}\pm\frac{1}{2}\delta$ 属于 R，因此 2 的确整除 $1+\delta$. 事实上，当 $d\equiv 1$(模 4)时，有更多的唯一因子分解的情形. 下面的定理非常深刻，我们将不加以证明.

【7.7】定理 *设 R 是虚二次域 $\mathbb{Q}[\sqrt{d}]$ 中的整数环. 则 R 是唯一因子分解整环当且仅当 d 是整数 $-1,\ -2,\ -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163$ 中的一个.*

高斯对 d 的这些值证明了 R 是唯一因子分解整环. 我们将学习是怎样证明的. 他还猜想没有其他的值. 定理中这一困难得多的部分在人们开始考虑它 150 年之后的 1966 年最终由贝克(Baker)和斯塔克(Stark)证明.

理想被引入来补救因数分解的唯一性. 如我们所知道的(2.12)，除非它是唯一因子分解整环，否则 R 必含有一些非主理想. 下一节将看到这些非主理想是如何替代元素的.

注意每个非零理想 A 是 R 的一个子格：它在加法之下是一个子群，并且由于 R 是离散的，它也是离散的. 还有，如果 α 是 A 的非零元，则 $\alpha\delta$ 亦属于 A，且 α，$\alpha\delta$ 在 $\mathbb{R}$ 上线性无关. 然而，并非每一子格都是一个理想.

【7.8】命题 *如果 $d\equiv 2$ 或 3(模 4)，则 R 的非零理想是在 δ 乘之下封闭的子格. 如果 $d\equiv 1$(模 4)，它们是在 $\eta=\frac{1}{2}(1+\delta)$ 乘之下封闭的子格.*

证明 一个子集要成为理想，就必须在加法和 R 中元素的乘之下封闭. 任意格在加法和整数的乘之下封闭. 因而如果它在 δ 乘之下封闭，则它在形如 $a+b\delta$(其中 $a,\ b\in\mathbb{Z}$)的元素的乘之下封闭. 如果 $d\equiv 2,\ 3$(模 4)，这便包括了 R 的所有元素. $d\equiv 1$(模 4)情形的证明是类似的. ■

为了对其可能性有个感觉，在继续讨论之前将描述环 $R=\mathbb{Z}[-5]$ 的理想. 最有意思的理想是那些不是主理想的理想.

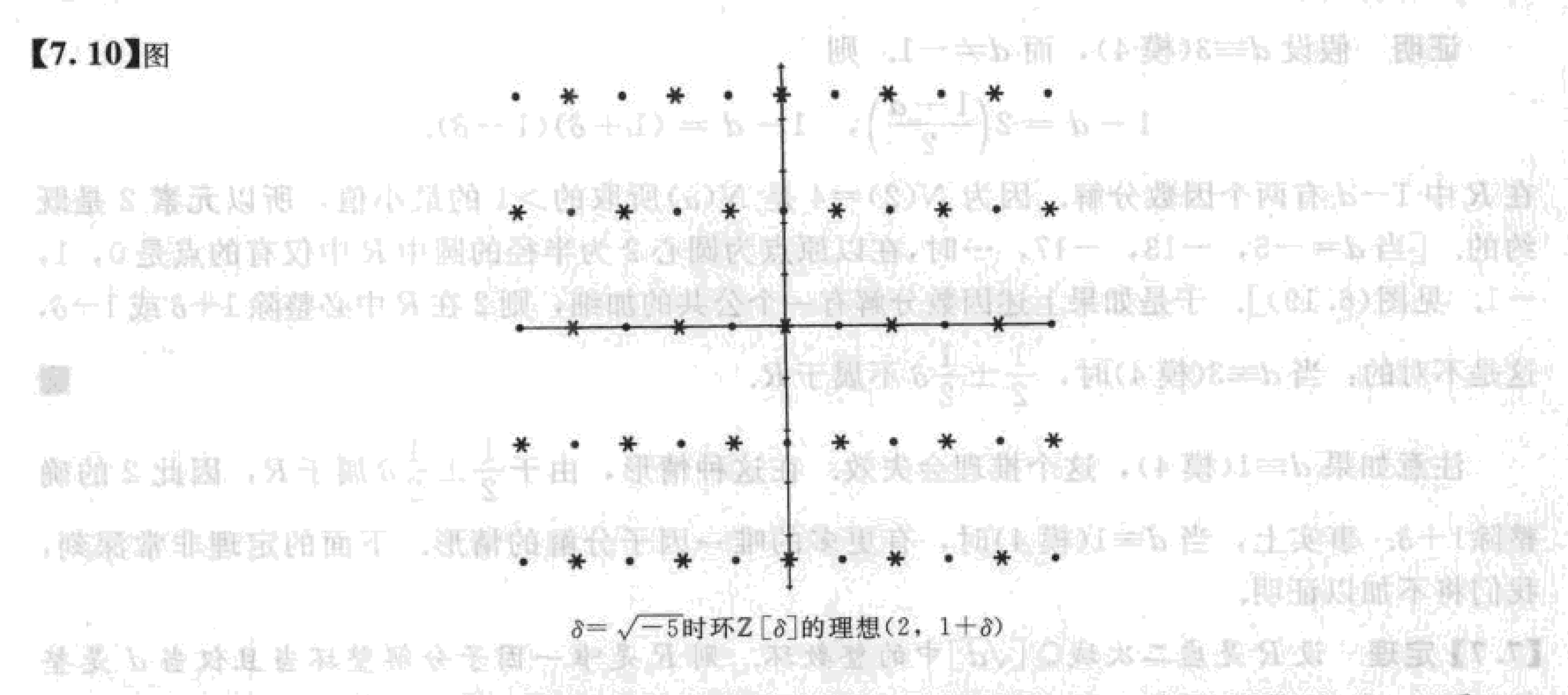
【7.9】定理 *设 $R=\mathbb{Z}[\delta]$，其中 $\delta=\sqrt{-5}$，并设 A 是 R 的非零理想. 设 α 是 A 的具有极小绝对值 $|\alpha|$ 的非零元素. 有下列两种情形：*

情形 1：A 是主理想，它有格基 $(\alpha,\ \alpha\delta)$.

情形 2：A 有格基 $\left(\alpha,\ \frac{1}{2}(\alpha+\alpha\delta)\right)$，且不是主理想.

第二种情形只有当元素 $\frac{1}{2}(\alpha+\alpha\delta)$ 属于 R 时才会发生. 作为例子，理想 $A=(2,\ 1+\delta)$ 图示如下.

【7.10】图



$\delta=\sqrt{-5}$时环$\mathbb{Z}[\delta]$的理想$(2,1+\delta)$

命题(7.9)的论断有一个几何解释. 注意主理想(α)的格基$(\alpha,\delta\alpha)$由R的格基$(1,\delta)$乘上α得到. 如果记$\alpha=re^{i\theta}$，则用α乘的效果是将复平面旋转过角度θ然后伸缩一个因子r. 因而(α)和R有相似的几何形状，如我们在第二节所见到的. 类似地，基$\left(\alpha,\frac{1}{2}(\alpha+\alpha\delta)\right)$由基$(2,1+\delta)$乘上$\frac{1}{2}\alpha$得到. 因而情形2列出的理想有与图(7.10)相似的几何图形. 理想的相似类称为理想类，其个数称为R的类数. 这样命题(7.9)蕴涵$\mathbb{Z}[\sqrt{-5}]$的类数为2. 我们将在第十节讨论其他虚二次域的理想类.

定理(7.9)的证明基于下列关于复平面上格的引理：

【7.11】引理　设r是一个格A中非零元素的极小绝对值，并设γ是A的元素. 设D是圆心在$\frac{1}{n}\gamma$半径为$\frac{1}{n}r$的圆盘. 除了其中心$\frac{1}{n}\gamma$外A中没有属于D的内部的点.

点$\frac{1}{n}\gamma$可以在A中也可以不在A中. 这依赖于A与γ.

证明　设β是D的内部的一个点. 则由圆盘的定义，$|\beta-\frac{1}{n}\gamma|<\frac{1}{n}r$，或等价地，$|n\beta-\gamma|<r$. 如果$\beta\in A$，则也有$n\beta-\gamma\in A$. 这时$n\beta-\gamma$是$A$中一个绝对值小于$r$的元素，这表明$n\beta-\gamma=0$，因此$\beta=\frac{1}{n}\gamma$. ■

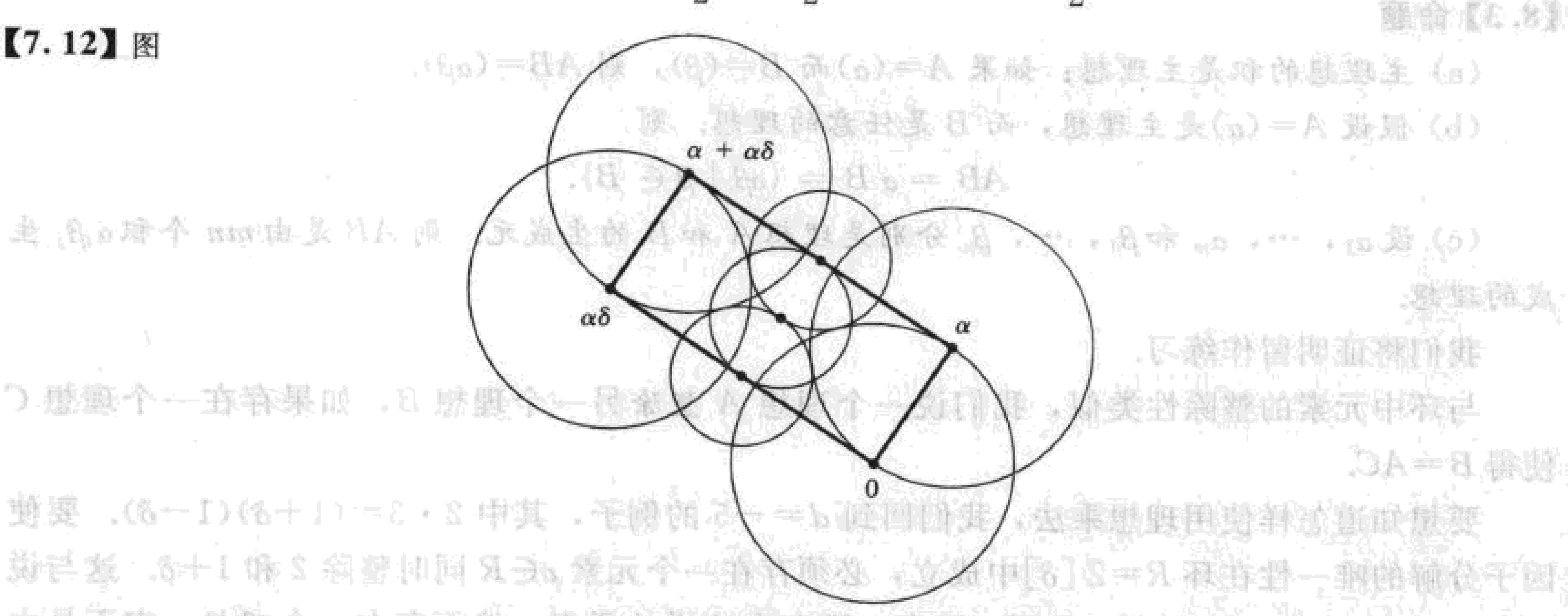
417

定理(7.9)的证明　设α是A中一个具有极小绝对值r的给定元素. 主理想$(\alpha)=R\alpha$由复数$(a+b\delta)\alpha$组成，其中$a,b\in\mathbb{Z}$. 因而它有如命题中所断言的格基$(\alpha,\delta\alpha)$. 由于A包含α，它也包含主理想(α)，且如果$A=(\alpha)$，我们得到情形1.

假设$A>(\alpha)$，并设β是A的不属于(α)的元素. 可将β取作位于四个顶点为$0,\alpha,\alpha\delta,\alpha+\alpha\delta$的长方形之中的点[见第五章(4.14)]. 图(7.12)表出这个长方形四个顶点上半径为r的圆盘以及在三个半格点$\frac{1}{2}\alpha\delta$，$\frac{1}{2}(\alpha+\alpha\delta)$和$\alpha+\frac{1}{2}\alpha\delta$上半径为$\frac{1}{2}r$的圆盘. 注意这些圆盘的内部

覆盖了长方形. 由引理(7.11)，圆盘的内部属于 A 的点仅有圆盘的中心. 由于 β 不属于(α)，故它不是长方形的顶点，因而 β 是半格点 $\frac{1}{2}\alpha\delta$，$\frac{1}{2}(\alpha+\alpha\delta)$ 和 $\alpha+\frac{1}{2}\alpha\delta$ 中的一个.

【7.12】 图



这用尽了由 A 是一个格这一事实所能得到的所有信息. 现在使用 A 是理想这一事实来排除两个点 $\frac{1}{2}\alpha\delta$ 和 $\alpha+\frac{1}{2}\alpha\delta$. 假设 $\frac{1}{2}\alpha\delta\in A$. 用 δ 乘，得到 $\frac{1}{2}\alpha\delta^2=-\frac{5}{2}\alpha\in A$，且由于 $\alpha\in A$，于是 $\frac{1}{2}\alpha\in A$. 这与 α 的选择矛盾. 其次，我们注意到如果 $\alpha+\frac{1}{2}\alpha\delta\in A$，则 $\frac{1}{2}\alpha$ 亦属于 A，但这已被排除掉. 剩下的可能性是 $\beta=\frac{1}{2}(\alpha+\alpha\delta)$. 如果这样，我们就得到了情形 2. ■

418

第八节 理想因子分解

设 R 是一个虚二次域的整数环. 为避免混乱，我们将用拉丁字母 a，b，…表示普通整数，用希腊字母 α，β，…表示 R 的元素，用大写字母 A，B，…表示理想. 我们只考虑 R 的非零理想.

记号 $A=(\alpha,\beta,\cdots,\gamma)$ 表示由元素 α，β，…，γ 生成的理想. 由于一个理想是一个平面格，它有由两个元素组成的格基. 任意格基生成这个理想，但必须区分格基与生成集合. 我们还需要回顾一下辞典(2.2)，它将元素与其生成的主理想联系起来.

戴德金(Dedekind)用下面的理想乘法的定义将可除性的概念拓广到理想：设 A 和 B 是环 R 中的理想. 我们希望定义积理想 AB 为所有积 $\alpha\beta$ 的集合，其中 $\alpha\in A$ 而 $\beta\in B$. 遗憾的是，这个积的集合通常不是一个理想：它在加法之下不封闭. 为得到理想，必须将所有积的有限和放到 AB 中

【8.1】
$$\sum_i \alpha_i\beta_i,\quad 其中\ \alpha_i\in A\ 而\ \beta_i\in B.$$

这样的和的集合是 R 中包含所有积 $\alpha\beta$ 的最小理想，将这个积理想记作 AB.（这里的积记号与它在群论中的用法不同[第二章(8.5)].）理想乘法的定义不像我们希望的那样简单，但它正好是我们想要的.

注意到理想的乘法是交换的和结合的，且 R 是一个单位元素. 这就是为什么 $R=(1)$ 常被

称为单位理想：

【8.2】 $$AR = RA = A,\quad AB = BA\quad A(BC) = (AB)C.$$

【8.3】命题

(a) 主理想的积是主理想：如果 $A=(\alpha)$ 而 $B=(\beta)$，则 $AB=(\alpha\beta)$.

(b) 假设 $A=(\alpha)$ 是主理想，而 B 是任意的理想. 则

$$AB = \alpha B = \{\alpha\beta \mid \beta \in B\}.$$

(c) 设 α_1，…，α_m 和 β_1，…，β_n 分别是理想 A 和 B 的生成元. 则 AB 是由 mn 个积 $\alpha_i\beta_j$ 生成的理想.

我们将证明留作练习.

与环中元素的整除性类似，我们说一个理想 A 整除另一个理想 B，如果存在一个理想 C 使得 $B=AC$.

要想知道怎样使用理想乘法，我们回到 $d=-5$ 的例子，其中 $2\cdot 3=(1+\delta)(1-\delta)$. 要使因子分解的唯一性在环 $R=\mathbb{Z}[\delta]$中成立，必须存在一个元素 $\rho\in R$ 同时整除 2 和 $1+\delta$. 这与说 2 和 $1+\delta$ 应该属于主理想(ρ)是同一回事. 不存在这样的元素. 然而存在一个理想，它不是主理想，包含 2 和 $1+\delta$，即由这两个元素生成的理想. 这个理想 $A=(2,1+\delta)$已在图(7.10)表示出来. 我们可以用 6 的因子做出其他三个理想：

419

$$\overline{A} = (2,1-\delta),\quad B = (3,1+\delta),\quad \overline{B} = (3,1-\delta).$$

这些理想中的第一个记作 $\overline{A}$ 是因为它是理想 A 的复共轭：

【8.4】 $$\overline{A} = \{\overline{\alpha} \mid \alpha \in A\}.$$

作为一个格，$\overline{A}$ 由格 A 关于实轴的反射得到. 容易看出任意理想的复共轭也是一个理想. 实际上我们的理想 A 恰好等于其复共轭 $\overline{A}$，因为 $1-\delta=2-(1+\delta)\in A$. 这是格 A 的一个偶然的对称：理想 B 与 $\overline{B}$ 是不相同的.

现在计算这些理想的积. 根据命题(8.3c)，理想 $A\overline{A}$ 由 A 和 $\overline{A}$ 的生成元$(2,1+\delta)$和$(2,1-\delta)$的生成元的四个乘积所生成：

$$A\overline{A} = (4, 2+2\delta, 2-2\delta, 6).$$

四个生成元中的每一个都能被 2 整除，于是 $A\overline{A}\subset(2)$. 另一方面，$2=6-4$ 属于 $A\overline{A}$. 因而$(2)\subset A\overline{A}$，这样

$$A\overline{A} = (2)!$$

[记号(2)是不明确的，因为它可既可以表示 $2\mathbb{Z}$ 又可表示 $2R$. 在这里它代表 $2R$.]其次，AB 由四个乘积

$$AB = (6, 2+2\delta, 3+3\delta, -4+2\delta)$$

生成. 这四个元素的每一个都能被 $1+\delta$ 整除. 由于 $1+\delta$ 属于 AB，我们得到 $AB=(1+\delta)$. 类似地，$\overline{AB}=(1-\delta)$，$B\overline{B}=(3)$.

由此得到主理想(6)是四个理想的积：

【8.5】 $$(6) = (2)(3) = (A\overline{A})(B\overline{B}) = (AB)(\overline{AB}) = (1+\delta)(1-\delta).$$

这不是很漂亮吗？理想因子分解$(6)=A\bar{A}B\bar{B}$给出(2.7)的两个因子分解的一个公共加细.

本节剩下的部分用于证明虚二次数域的整数环的理想的唯一因子分解. 我们将尽可能地按元素因子分解的讨论来进行.

首先要对理想找出类似的素元素的概念.

【8.6】命题 设P是环R的一个不是单位理想的理想. 则下列条件是等价的:

(i) 如果α, β是R中元素且$\alpha\beta\in P$, 则$\alpha\in P$或$\beta\in P$.

420

(ii) 如果A, B是R的理想且$AB\subset P$, 则$A\subset P$或$B\subset P$.

(iii) 商环R/P是整环.

满足这些条件之一的理想称为一个素理想.

例如, 每个极大理想是素的, 因为如果M是极大的, 则R/M是域, 而域是整环. 环R的零理想是素理想当且仅当R是整环.

命题的证明 使$\bar{R}=R/P$为整环的条件是$\bar{R}\neq 0$且由$\bar{\alpha}\bar{\beta}=0$得到$\bar{\alpha}=0$或$\bar{\beta}=0$. 这些条件翻译回来就是$P\neq R$以及如果$\alpha\beta\in P$, 则$\alpha\in P$或$\beta\in P$. 这样(i)与(iii)是等价的. 取$A=(\alpha)$和$B=(\beta)$可以看到(ii)蕴涵(i)这一事实. 仅有的令人惊讶的蕴涵关系是(i)蕴涵(ii). 假设(i)成立, 并设A, B是使得$AB\subset P$的理想. 如果A不含于P, 存在某个元素$\alpha\in A$, 但它不属于P. 如果β是B的元素, 则$\alpha\beta\in AB$; 因此$\alpha\beta\in P$. 由(i)得$\beta\in P$. 由于这对其所有元素成立, 故$B\subset P$, 这正是要证的. ■

我们现在回到虚二次数域.

【8.7】引理 设$A\subset B$是$\mathbb{R}^2$的格. 只有有限多个格L介于A与B间, 即满足$A\subset L\subset B$.

证明 设(α_1, α_2)是A的格基, 并设P是以0, α_1, α_2, $\alpha_1+\alpha_2$为顶点的平行四边形. 有有限多个B的元素包含于P[第五章(4.12)], 因而如果L是A和B之间的格, 集合$L\cap P$便有有限多种可能性. 将这个集合称为S. 通过证明S和A确定格L就可完成证明. 为此, 设γ为L的一个元素. 则存在元素$\alpha\in A$使得$\gamma-\alpha$属于P, 因此也属于S. [见第五章中(4.14)的证明]. 从符号上, 我们得到$L=S+A$. 这正是需要的用S和A对L的描述. ■

【8.8】命题 设R是虚二次数域的整数环.

(a) 设B是R的非零理想. 在B与R之间有有限多个理想.

(b) R的每个真理想含在一个极大理想中.

(c) R的非零素理想是极大理想.

证明

(a) 这可由引理(8.7)得到.

(b) 设B是真理想. 则B仅包含在有限多个理想之中. 我们可搜遍它们而找到一个极大理想.

(c) 我们已经注意到极大理想是素的. 反之, 设P是非零素理想. 则P在R中的指标有限. 因而R/P是一个有限整环, 因此它是域[第十章(6.10)]. 这表明P是极大理想. ■

421

【8.9】定理 设R是虚二次域F中的整数环. R的每一个不是整个环的非零理想是素理想的积. 这个因子分解除了因子的顺序外是唯一的.

这一引人注目的定理可以拓广到其他的代数整数环，但它是这样的环的非常特殊的一个性质．大多数环没有理想的唯一因子分解．有几个要求得不到满足，我们想要特别注意其中之一．我们知道一个主理想(α)包含另一个主理想(β)当且仅当在环中α整除β．因而素元素π的定义可复述如下：如果$(\pi)\supset(\alpha\beta)$，则$(\pi)\supset(\alpha)$或$(\pi)\supset(\beta)$．素理想等价定义(8.6)的第二条是对理想的类似陈述：如果$P\supset AB$，则$P\supset A$或$P\supset B$．因而如果理想的包含等价于整除性，那么因子分解的唯一性的证明就可以搬到理想上．遗憾的是理想乘积的笨拙定义引起了麻烦．在大多数环中，包含$A\supset B$并不意味着A整除B．这就减弱了素理想与素元素间的相似性．重要的是在我们所研究的特殊的环上建立包含与可除性的等价关系．在下面的命题(8.11)中做到了这一点．

现在着手证明定理(8.9)．在本节剩下的部分，R将表示虚二次数域中的整数环．证明基于下面的引理．

【8.10】主要引理 *设R是虚二次数域中的整数环．一个非零理想与其共轭的积是由普通整数生成的R的主理想：*

$$\text{存在 } n\in\mathbb{Z}\text{，使得}\quad A\overline{A}=(n).$$

这里最重要的一点是对每个理想A，存在某个理想B使得AB为主理想．$\overline{A}$起到这个作用和主理想是由一个普通整数生成都不是那么重要．

我们将在本节最后证明这个引理．现在假设它成立并导出理想乘法的一些结果．由于这些结果依赖于主要引理，对一般环它们不成立．

【8.11】命题 *设R是虚二次数域中的整数环．*

(a) 消去律：设A，B，C是R的非零理想．如果$AB\supset AC$则$B\supset C$．如果$AB=AC$则$B=C$．

(b) 如果A和B是R的非零理想，则$A\supset B$当且仅当A整除B，即当且仅当存在理想C使得$B=AC$．

(c) 设P是R的非零素理想．如果P整除理想的乘积AB，则P整除其因子A或B之一．

证明 (a) 假定$AB\supset AC$．如果$A=(\alpha)$为主理想，则$AB=\alpha B$而$AC=\alpha C$(8.3)．将这些集合视为复数的子集，在关系$\alpha B\supset\alpha C$的左边乘上α^{-1}而得到$B\supset C$．因而当A是主理想时断言成立．一般地，如果$AB\supset AC$，则两边乘上$\overline{A}$并应用主要引理：$nB=\overline{A}AB\supset\overline{A}AC=nC$，并应用已证部分即可得证．$AB=AC$的情形是同样的．

(b) 不清楚的地方是如果A包含B则A整除B．首先检验当$A=(\alpha)$为主理想的情形．在这一情形，说$(\alpha)\supset B$也就是说α整除B的每个元素β．设$C=\alpha^{-1}B$为商的集合，即元素$\alpha^{-1}\beta$的集合，其中$\beta\in B$．可以验证C是一个理想且$\alpha C=B$．因而在这一情形有$B=AC$．现设A是任意的，并设$A\supset B$．则$(n)=\overline{A}A\supset\overline{A}B$．由已证明的部分得到存在理想$C$使得$nC=\overline{A}B$，或$\overline{A}AC=\overline{A}B$．由消去律，$AC=B$．

要证明(c)，我们应用(b)将可除性翻译为包含．则(c)由素理想的定义得到．■

定理(8.9)的证明 有两点要证明．首先要证每一个真的非零理想A是素理想的积．如果A本身不是素的，则它不是极大的，因而可以找到严格大于A的真理想A_1．则A_1整除A(8.11b)，因而可以记$A=A_1B_1$．由此得到$A\subset B_1$．而且如果有$A=B_1$，则消去律给出$R=$

A_1，这与 A_1 是真理想这一事实矛盾．这样 $A<B_1$．类似地有 $A<A_1$．由于 A 与 R 之间只存在有限多个理想，理想的这个因子分解过程终止．这时所有因子都将是极大的，因此也都是素的．因而每个真理想 A 可以因子分解为素理想．

现在证明唯一性，应用素理想的性质(8.11c)：如果 $P_1\cdots P_r=Q_1\cdots Q_s$，且 P_i，Q_j 为素的，则 P_1 整除 $Q_1\cdots Q_s$，因此它整除这些因子中的一个，比如说 Q_1．由于 Q_1 极大，$P_1=Q_1$．由(8.11a)消去它并对 r 归纳即可得证． ■

【8.12】定理 整数环 R 是唯一因子分解整环当且仅当它是主理想整环．这时，元素的因数分解与理想的因子分解自然地对应．

证明 我们已经知道主理想整环有唯一因子分解(2.12)．反之，假设 R 是唯一因子分解整环，并设 P 是 R 的任一非零素理想．则 P 包含一个既约元，设为 π．因为 P 中任意元素 α 都是既约元的积，且由素理想的定义，P 包含其既约因子中的一个．由(2.8)，既约元 π 是素的，即(π)是素理想．由(8.6)，(π)是极大的．由于$(\pi)\subset P$，由此得$(\pi)=P$，因此 P 是主理想．由定理(8.9)，每个非零理想 A 是素理想的积；因此它是主理想(8.3a)．这样 R 是主理想整环．由(2.2)，定理的最后的断言是显然成立的． ■

423

主要引理(8.10)的证明 可以把 A 作为由两个元素，如 α，β 生成的格．则 A 当然也是由这两个元素生成的理想，且$\bar{\alpha}$，$\bar{\beta}$生成 $\bar{A}$．因此四个积 $\alpha\bar{\alpha}$，$\alpha\bar{\beta}$，$\bar{\alpha}\beta$，$\beta\bar{\beta}$ 生成理想 $A\bar{A}$．考虑 $A\bar{A}$ 的三个元素 $\alpha\bar{\alpha}$，$\beta\bar{\beta}$ 和 $\alpha\bar{\beta}+\bar{\alpha}\beta$．它们都等于其共轭，因此是有理数．由于它们是代数整数，因而它们必为普通的整数．设 n 是它们在$\mathbb{Z}$中的最大公因数．于是 n 是 $\alpha\bar{\alpha}$，$\beta\bar{\beta}$，$\alpha\bar{\beta}+\bar{\alpha}\beta$ 的整系数线性组合．因此 n 属于积理想 $A\bar{A}$．于是 $A\bar{A}\supset(n)$．如果证明 n 整除 R 中的理想 $A\bar{A}$ 的生成元中的每一个，则由此将得到$(n)\supset A\bar{A}$，因此$(n)=A\bar{A}$，这正是要证的．

现由构造，在$\mathbb{Z}$中因而也在 R 中有 n 整除 $\alpha\bar{\alpha}$ 和 $\beta\bar{\beta}$．因此需要证明在 R 中 n 整除 $\alpha\bar{\beta}$ 和 $\bar{\alpha}\beta$．元素$(\alpha\bar{\beta})/n$ 和$(\bar{\alpha}\beta)/n$ 是多项式 x^2-rx+s 的根，其中

$$r=\frac{\alpha\bar{\beta}+\bar{\alpha}\beta}{n} \quad 及 \quad s=\frac{\alpha\bar{\alpha}}{n}\frac{\beta\bar{\beta}}{n}.$$

由 n 的定义，这两个元素 r，s 为整数，因而这是$\mathbb{Z}[x]$中的首一多项式．因此$(\alpha\bar{\beta})/n$ 和$(\bar{\alpha}\beta)/n$ 是代数整数，这正是要证的． ■

注 只有这里是直接用到代数整数定义的地方．如果取一个比 R 更小的环，例如，当 $d\equiv 1$(模 4)时不取系数为半整数的元素时引理将会不成立．

第九节 R 的素理想与素整数的关系

在第五节中我们看到高斯整数环中的素元素是如何与素整数联系起来的．对二次数域中的整数环 R 可作类似的分析．主要的区别是 R 通常不是一个主理想整环，因而应该讲素理想而不是素元素．这使得定理(5.1)的(c)和(d)的类似变得复杂，我们将不在此加以考虑．[但可参见(12.10).]

【9.1】命题 设 P 是 R 的非零素理想．存在一个整素数 p 使得要么 $P=(p)$要么 $P\bar{P}=(p)$．反

之，设 p 是一个素整数．存在 R 的素理想 P 使得要么 $P=(p)$ 要么 $P\bar{P}=(p)$．

424 证明可按定理(5.1)中(a)和(b)的证明直接进行．

(9.1)中的第二种情形根据 P 与 $\bar{P}$ 是否相等，又分为两种情形．习惯上用下面的术语：如果(p)是素理想，则说 p 在 R 中保持素性．如果 $P\bar{P}=(p)$，则当 $P\neq\bar{P}$ 时说 p 在 R 中分裂，而在 $P=\bar{P}$ 时说 p 在 R 中分歧．

我们进一步分析素数的特性．假设 $d\equiv 2$ 或 3(模 4)．在这一情形，$R=\mathbb{Z}[\delta]$与$\mathbb{Z}[x]/(x^2-d)$同构．求包含(p)的素理想等价于求环 $R/(p)$的素理想[第十章(4.3)]．注意

【9.2】
$$R/(p)\approx\mathbb{Z}[x]/(x^2-d,p).$$

如在定理(5.1)的证明中同样交换两个关系 $x^2-d=0$ 和 $p=0$ 的顺序，我们得到下面命题的第一部分．应用多项式(6.16)，第二部分可用同样的方法得到．

【9.3】命题

(a) 假设 $d\equiv 2$ 或 3(模 4)．一个整素数 p 在 R 中保持素性当且仅当多项式 x^2-d 在$\mathbb{F}_p$ 上既约．

(b) 假设 $d\equiv 1$(模 4)．则 p 保持素性当且仅当多项式 $x^2-x+\frac{1}{4}(1-d)$在$\mathbb{F}_p$ 上既约．

第十节　虚二次域的理想类

如同前面一样，R 表示一个虚二次数域中的整数环．为了分析 R 中元素的因数分解唯一性的失效程度，我们引入理想的一个等价关系，它与理想乘法相容并且使得主理想构成一个等价类．使用哪个等价关系是相当明显的：我们称两个理想 A，B 是相似的，如果存在非零元素 σ，$\tau\in R$ 使得

【10.1】
$$\sigma B=\tau A.$$

这是一个等价关系．这个关系的等价类称为理想类，A 的理想类记为$\langle A\rangle$．

我们也可在二次数域 $F=\mathbb{Q}[\delta]$中取元素 $\lambda=\sigma^{-1}\tau$并称 A 和 B 是相似的，如果

【10.2】
$$\text{存在}\quad \lambda\in\mathbb{Q}[\delta]\quad\text{使得}\quad B=\lambda A.$$

相似性有一个很好的几何解释．两个理想 A 和 B 是相似的，如果复平面上代表它们的格有相似的几何形状，这可通过一个保向的相似来实现．要看到这一点，注意一个格在所有点处都是一样的．因而可以假设相似性将 A 的 0 与 B 的 0 联系起来．于是它将被描述为一个旋转加上一个伸展或收缩，也就是乘上一个复数 λ．由于乘上 λ 将非零元素 $\alpha\in A$ 变为 $\lambda\alpha=\beta\in B$，

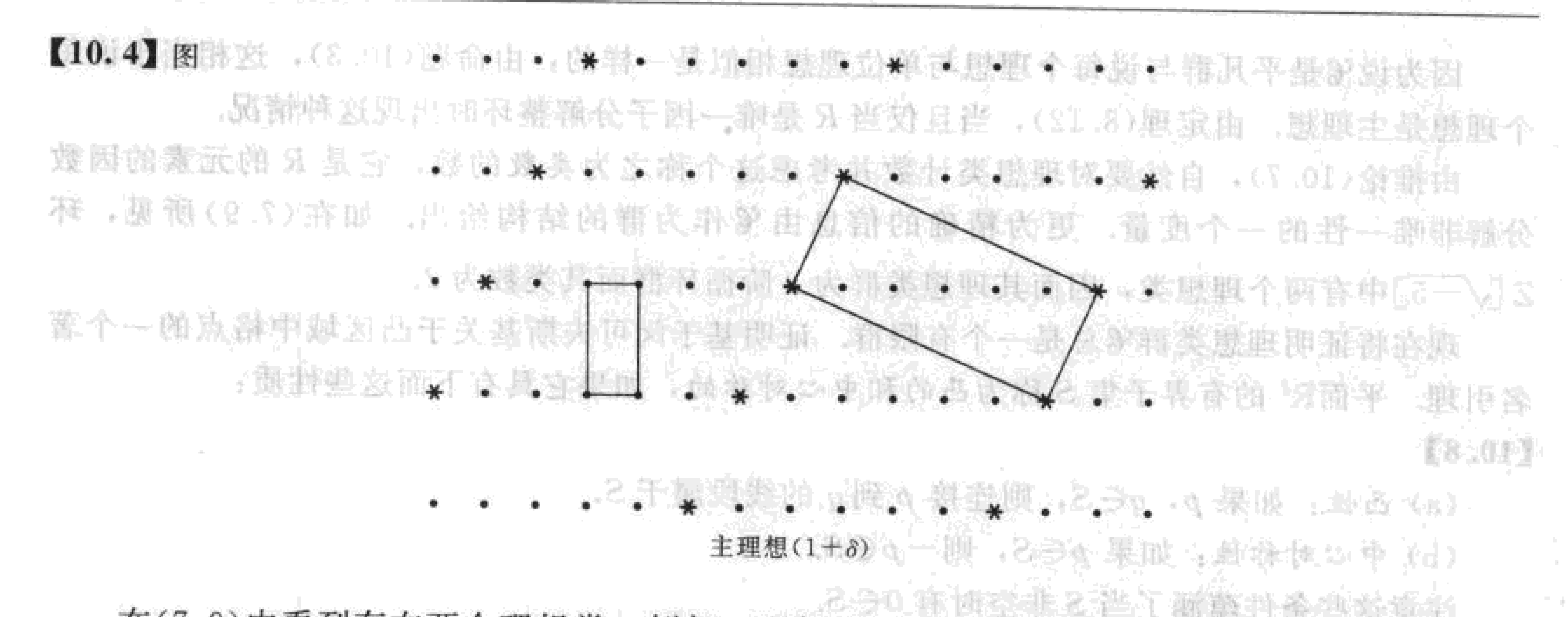
425 $\lambda=\beta\alpha^{-1}$自然也是属于域 F 的．

一个理想 B 与单位理想 R 相似当且仅当对域中某个元素 λ 有 $B=\lambda R$．于是 λ 是 B 的元素，因而也是 R 的元素．这时 B 是主理想(λ)．于是我们有下面的命题：

【10.3】命题　理想类$\langle R\rangle$由主理想组成．

图(10.4)表示环$\mathbb{Z}[\delta]$的主理想$(1+\delta)$，其中 $\delta^2=-5$．

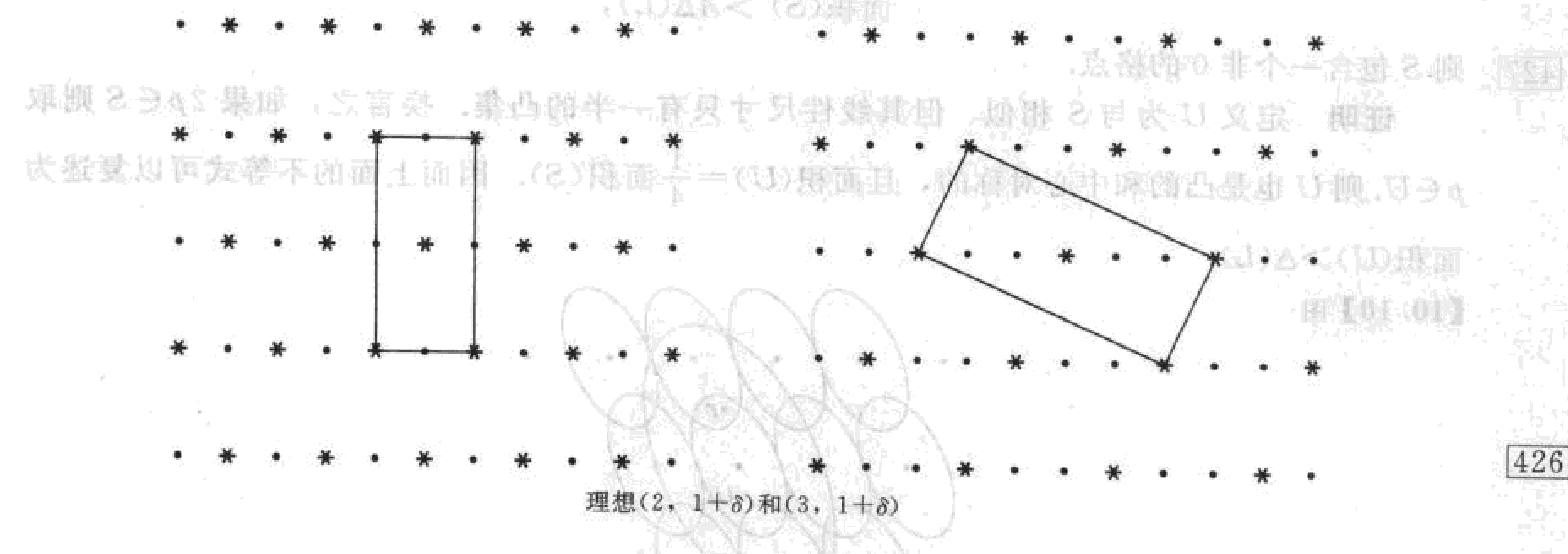
【10.4】图



主理想$(1+\delta)$

在(7.9)中看到存在两个理想类，例如，理想$A=(2,1+\delta)$和$B=(3,1+\delta)$中的每一个都代表非主理想类. 这时$2B=(1+\delta)A$. 这些理想如图(10.5)所示.

【10.5】图



理想$(2,1+\delta)$和$(3,1+\delta)$

426

【10.6】命题 理想类构成一个阿贝尔群$\mathscr{C}$，其合成法则由理想的乘法导出：

$$\langle A\rangle\langle B\rangle = AB \text{ 的类} = \langle AB\rangle;$$

主理想的类是单位元$\langle R\rangle=\langle 1\rangle$.

证明 如果$A\sim A'$并且$B\sim B'$，则存在$\lambda,\mu\in F=\mathbb{Q}[\delta]$，使得$A'=\lambda A$和$B'=\mu B$成立；因此$A'B'=\lambda\mu AB$. 这证明了$\langle AB\rangle=\langle A'B'\rangle$，因而合成法则是唯一定义的. 其次，因为理想的乘法是交换的和结合的，该法则也是交换的和结合的，且R的类是单位元(8.2). 最后，由主要引理(8.10)，$A\overline{A}=(n)$是主理想. 由于主理想(n)的类是$\mathscr{C}$中的单位元，我们有$\langle A\rangle\langle\overline{A}\rangle=\langle R\rangle$，因而$\langle\overline{A}\rangle=\langle A\rangle^{-1}$. ■

【10.7】推论 设R是一个虚二次数域中的整数环. 下列断言等价：

(i) R是主理想整环.

(ii) R是唯一因子分解整环.

(iii) R的理想类群$\mathscr{C}$是平凡群.

因为说$\mathscr{C}$是平凡群与说每个理想与单位理想相似是一样的，由命题(10.3)，这相当于说每个理想是主理想．由定理(8.12)，当且仅当R是唯一因子分解整环时出现这种情况．

由推论(10.7)，自然要对理想类计数并考虑这个称之为类数的数，它是R的元素的因数分解非唯一性的一个度量．更为精确的信息由$\mathscr{C}$作为群的结构给出．如在(7.9)所见，环$\mathbb{Z}[\sqrt{-5}]$中有两个理想类，因而其理想类群为2阶循环群而其类数为2.

现在将证明理想类群$\mathscr{C}$总是一个有限群．证明基于闵可夫斯基关于凸区域中格点的一个著名引理．平面$\mathbb{R}^2$的有界子集S称为凸的和中心对称的，如果它具有下面这些性质：

【10.8】

(a) 凸性：如果p，$q\in S$，则连接p到q的线段属于S.

(b) 中心对称性：如果$p\in S$，则$-p\in S$.

注意这些条件蕴涵了当S非空时有$0\in S$.

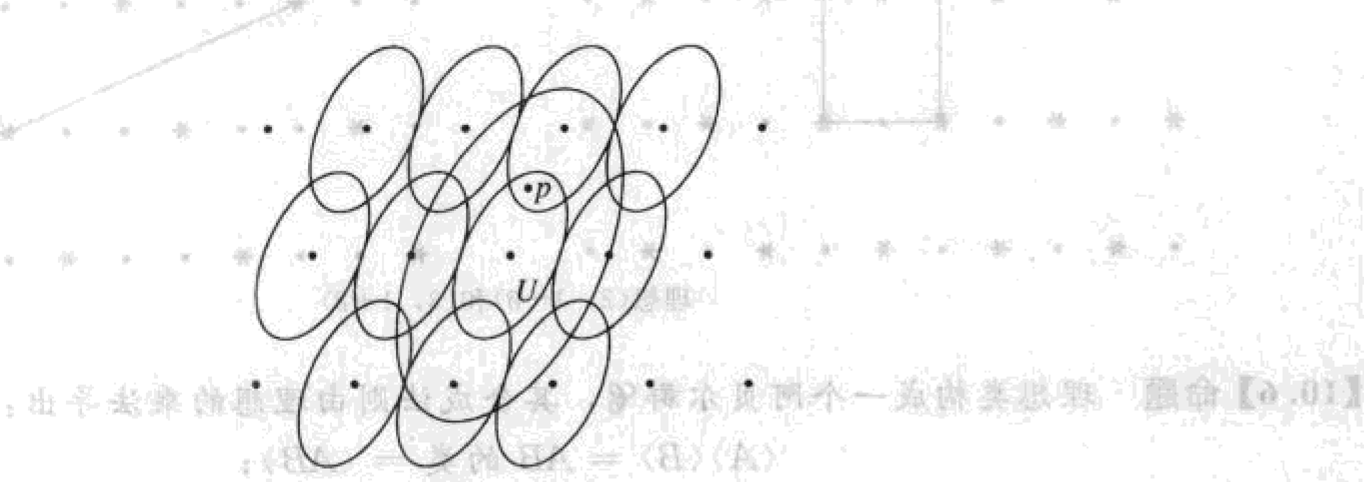
【10.9】闵可夫斯基引理 设L是$\mathbb{R}^2$的格，并设S在$\mathbb{R}^2$中为凸的、中心对称的子集．用$\Delta(L)$表示由L的一个格基张成的平行四边形的面积．如果

$$\text{面积}(S) > 4\Delta(L),$$

427 则S包含一个非0的格点．

证明 定义U为与S相似、但其线性尺寸只有一半的凸集．换言之，如果$2p\in S$则取$p\in U$. 则U也是凸的和中心对称的，且面积$(U)=\frac{1}{4}$面积(S)．因而上面的不等式可以复述为面积$(U)>\Delta(L)$.

【10.10】图



【10.11】引理 *存在元素$\alpha\in L$使得$U\cap(U+\alpha)$非空.*

证明 设P是由L的一个格基张成的平行四边形．则由$\alpha\in L$得到的平移$P+\alpha$覆盖了平面，且除了其边之外没有重叠．引理成立的一个有启发的原因是：对每个平移$P+\alpha$，存在一个平移$U+\alpha$，且U的面积比P的面积大．因而平移$U+\alpha$必将重叠．为使之更精确一些，我们注意到由于U是有界集，它与有限多个平移$P+\alpha$相交，比如它与$P+\alpha_1$，…，$P+\alpha_k$相交．用U_i记集合$(P+\alpha_i)\cap U$．则U被切成小块U_1，…，U_k，且面积$(U)=\sum$面积(U_i)．通过减去α_i可将U_i平移回到P，令$V_i=U_i-\alpha_i$，我们注意到$V_i=P\cap(U-\alpha_i)$．因而V_i是P的子集，且面积$(V_i)=$面积(U_i)．于是$\sum$面积$(V_i)=$面积$(U)>\Delta(L)=$面积(P)．这蕴涵集合V_i中的必有两个相交，即存在某个$i\neq j$使得$(U-\alpha_i)\cap(U-\alpha_j)$非空．加上$\alpha_i$并令$\alpha=\alpha_i-\alpha_j$，我们得到$U\cap(U+\alpha)$也非空． ■

回到闵可夫斯基引理的证明，如引理(10.11)中那样选择 α，并设 p 是 $U\cap(U+\alpha)$ 的一个点．由 $p\in U+\alpha$ 可得 $p-\alpha\in U$．由中心对称性，也有 $q=\alpha-p\in U$．因为 U 是凸的，p，q 间的中点 $\frac{1}{2}\alpha$ 也属于 U．因而 $\alpha\in S$，这正是要证的． ■

【10.12】推论 $\mathbb{R}^2$ 的任意格 L 含有一个非零向量 α 满足

$$|\alpha|^2\leqslant 4\Delta(L)/\pi.$$

428

证明 我们应用闵可夫斯基引理，取 S 为以原点为圆心 r 为半径的圆．引理保证了当 $\pi r^2>4\Delta(L)$ 或 $r^2>4\Delta(L)/\pi$ 时，S 中存在一个非零格点．因而对任意整数 ε，存在格点 α 使得 $|\alpha|^2<4\Delta(L)/\pi+\varepsilon$．由于在一个有界区域里只有有限多个格点并且由于 ε 可以任意小，因此存在一个满足我们所要求的不等式的格点． ■

现在转到虚二次域中的整数环 R 的理想．对一个理想的大小有两个度量，它们是一样的．第一个是理想在 R 中的指标．由于一个理想 A 是 R 的子格，它的指标有限：

$$[R:A]=A\text{ 在 }R\text{ 中加法陪集的个数}.$$

指标可以用由基向量张成的平行四边形的面积表出：

【10.13】引理 设(a_1,a_2)及(b_1,b_2)为$\mathbb{R}^2$ 中的格 $B\supset A$ 的格基，并设 $\Delta(A)$ 及 $\Delta(B)$ 是由这些基张成的平行四边形的面积．则$[B:A]=\Delta(A)/\Delta(B)$．

我们将证明留作练习．

【10.14】推论

(a) 设 A 是一个平面格．则面积 $\Delta(A)$ 与 A 的格基无关．

(b) 如果 $C\supset B\supset A$ 是格，则$[C:A]=[C:B][B:A]$．

用环的描述(6.14)容易计算面积 $\Delta(R)$：

【10.15】
$$\Delta(R)=\frac{1}{2}\sqrt{|D|}=\begin{cases}\sqrt{|d|} & \text{如果 } d\equiv 2,3(\text{模 }4)\\ \frac{1}{2}\sqrt{|d|} & \text{如果 } d\equiv 1(\text{模 }4)\end{cases},$$

其中 D 是判别式(6.18)．

理想大小的另一个度量可由主要引理(8.10)得到：记 $A\overline{A}=(n)$ 并取整数 n（当然选择>0的）．这与元素的范数(7.1)是类似的，因而称之为理想的范数：

【10.16】
$$N(A)=n,\quad \text{如果 } A\overline{A}=(n).$$

它具有乘法性质

【10.17】
$$N(AB)=N(A)N(B),$$

因为如果 $N(B)=m$，则 $AB\overline{AB}=A\overline{A}B\overline{B}=(nm)$．另外注意如果 A 是主理想(α)，则其范数为 α 的范数：因为$(\alpha)(\overline{\alpha})=(\alpha\overline{\alpha})$，所以

429

【10.18】
$$N((\alpha))=\alpha\overline{\alpha}=N(\alpha).$$

【10.19】引理 对 R 的任意非零理想 A，

$$[R:A]=N(A).$$

【10.20】推论 指标的乘法性质：设 A 和 B 是 R 的非零理想．则

$$[R:AB]=[R:A][R:B].$$

我们把引理(10.19)的证明放到后面而先由它导出类数的有限性.

【10.21】定理 设$\mu=2\sqrt{|D|}/\pi$. 每个理想类包含一个理想A使得$N(A)\leqslant\mu$.

证明 设A是一个理想. 我们需要在A的类中找到范数不大于μ的另一个理想A'. 应用推论(10.12)：存在一个元素$\alpha\in A$使得

$$N(\alpha)=|\alpha|^2\leqslant 4\Delta(A)/\pi.$$

于是$A\supset(\alpha)$. 这表明A整除(α)，即对某个理想C有$AC=(\alpha)$. 由范数的乘法性质(10.17)并由(10.18)，$N(A)N(C)=N(\alpha)\leqslant 4\Delta(A)/\pi$. 用(10.13)、(10.14)和(10.19)，可记$\Delta(A)=[R:A]\Delta(R)=\frac{1}{2}N(A)\sqrt{|D|}$. 代入$\Delta(A)$并消去$N(A)$，我们得$N(C)\leqslant\mu$.

由于CA是主理想，类$\langle C\rangle$是$\langle A\rangle$的逆，即$\langle C\rangle=\langle\overline{A}\rangle$. 因而我们证明了$\langle\overline{A}\rangle$包含一个范数满足所需不等式的理想. 交换$A$与$\overline{A}$的角色就完成了证明. ■

容易得到类数的有限性.

【10.22】定理 理想类群$\mathscr{C}$是有限的.

证明 因为(10.19)及(10.21)，只要证明有有限多个使指标$[R:A]\leqslant\mu$的理想就行了，因而只需证明仅有有限多个使得$[R:L]\leqslant\mu$的子格$L\subset R$. 选择一个整数$n\leqslant\mu$并设L是使得$[R:L]=n$的子格. 则R/L是一个n阶阿贝尔群，因而在这个群上用n乘是零映射. 这个事实在R上翻译成$nR\subset L$：指标为n的子格包含nR. 引理(8.7)表明有有限多个这样的格L. 由于n也有有限多种可能，定理得证. ■

可以通过检验哪个指标$\leqslant\mu$的子格$L\subset R$是理想来具体地计算理想类群. 然而，这样做效率不高. 最好是直接寻找素理想. 用$[\mu]$表示不大于μ的最大整数.

【10.23】命题 理想类群$\mathscr{C}$由整除素整数$p\leqslant[\mu]$的素理想P的类生成.

证明 我们知道每一类包含一个范数$N(A)\leqslant\mu$的理想A，并且由于$N(A)$是整数，$N(A)\leqslant[\mu]$. 假设一个范数$\leqslant\mu$的理想A分解为素理想的积：$A=P_1\cdots P_r$. 则由(10.17)，$N(A)=N(P_1)\cdots N(P_r)$. 因此对每个i有$N(P_i)\leqslant[\mu]$. 于是范数$\leqslant[\mu]$的素理想P的类构成$\mathscr{C}$的生成元集，这正是我们所断言的. ■

要应用这个命题，我们检查每个素整数$p\leqslant[\mu]$. 如果p在R中保持素性，则素理想(p)是主理想，因而其类是平凡的. 我们丢掉这些素数. 如果p在R中不是素数，则将其两个素理想类中的一个包括在我们的生成元集中. 另一个素因子的类是其逆. P仍然可能是主理想，在这种情形我们就丢掉它. 剩下的素理想生成$\mathscr{C}$.

表(10.24)给出一些值来说明不同的群.

【10.24】表 **一些理想类群**

d	D	$[\mu]$	理想类群
-2	-8	1	平凡
-5	-20	2	2 阶
-13	-52	4	2 阶
-14	-56	4	4 阶，循环

（续）

d	D	$[\mu]$	理想类群
-21	-84	5	克莱因四元群
-23	-23	3	3 阶
-26	-104	6	6 阶
-47	-47	4	5 阶
-71	-71	5	7 阶

【10.25】例 为应用命题(10.23)，对所有素整数 $p\leqslant\mu$ 将(p)因子分解为素理想.

(a) $d=-7$. 在这一情形$[\mu]=1$. 命题(10.23)告诉我们类群$\mathscr{C}$由素理想的空集生成. 因而$\mathscr{C}$是平凡的，并且 R 是唯一因子分解整环.

(b) $d=-67$. 这里 $R=\mathbb{Z}[\eta]$，其中 $\eta=\frac{1}{2}(1+\delta)$，且$[\mu]=5$. 理想类群由整除 2，3，5 的素理想生成. 根据命题(9.3)，一个素整数 p 在 R 中仍为素整数当且仅当多项式 x^2-x+17 模 p 是既约的. 这对素数 2，3，5 中的每一个都成立. 因而所涉及的素理想都是主理想，于是理想类群是平凡的.

(c) $d=-14$. 这里$[\mu]=4$，因而$\mathscr{C}$由整除(2)和(3)的素理想生成. 多项式 x^2+14 模 2 和模 3 都是可约的，因而由(9.3)，这些整数在 R 中都不再是素的. 设$(2)=P\overline{P}$ 和$(3)=Q\overline{Q}$. 如对$\mathbb{Z}[\sqrt{-5}]$的讨论一样，我们得到 $P=(2,\delta)=\overline{P}$. 理想类$\langle P\rangle$在$\mathscr{C}$中的阶为 2.

431

要计算类$\langle Q\rangle$的阶，可以具体计算理想的幂并求出其格与 R 相似的第一个幂. 这样做效率不高. 最好是计算 R 的一些小元素的范数，从而希望从中推导出其生成元间的关系. 最为明显的可用元素是 δ 和 $1+\delta$. 但 $N(\delta)=14$ 而 $N(1+\delta)=15$. 它们没有我们所希望的那么好，因为它们涉及素数 5 和 7，其因数不在我们的生成元之列. 我们不愿让这些额外的素数搅进来. 元素 $2+\delta$ 更好些：$N(2+\delta)=(2+\delta)(2-\delta)=2\cdot 3\cdot 3$. 这给出了理想的关系

$$(2+\delta)(2-\delta)=P\overline{P}Q\overline{Q}Q\overline{Q}=P^2Q^2\overline{Q}^2.$$

由于 $2+\delta$ 与 $2-\delta$ 不相伴，它们不能生成同一个理想. 另一方面，它们生成相互共轭的两个理想. 考虑到这些事实，$(2+\delta)$仅有的素因子分解为 PQ^2 或 $P\overline{Q}^2$. 是哪种情形依赖于将(3)的哪个因子标为 Q. 这样可假设$(2+\delta)=PQ^2$. 则由于$(2+\delta)$是主理想，在$\mathscr{C}$中$\langle P\rangle\langle Q\rangle^2=1$. 因而$\langle Q\rangle^2=\langle P\rangle^{-1}=\langle P\rangle$. 这表明$\mathscr{C}$是由$\langle Q\rangle$生成的 4 阶循环群.

(d) $d=-23$，因此 $R=\mathbb{Z}[\eta]$，其中 $\eta=\frac{1}{2}(1+\delta)$. 于是$[\mu]=3$，因而$\mathscr{C}$由整除(2)和(3)的素理想的类生成. 因为多项式 x^2-x+6 模 2 和模 3 都可约(9.3)，这两个素数都在 R 中分裂. 事实上，$(2)=P\overline{P}$，其中 P 具有格基$(2,\eta)$[见(7.8)]. 这不是一个主理想.

设$(3)=Q\overline{Q}$. 为确定理想类群的结构，我们注意到 $N(\eta)=2\cdot 3$ 而 $N(1+\eta)=2\cdot 2\cdot 2$. 因而

$$(\eta)(\overline{\eta})=P\overline{P}Q\overline{Q}\quad 并且\quad (1+\eta)(\overline{1+\eta})=(8)=(2)^3=P^3\overline{P}^3.$$

必要时交换 P 与 $\overline{P}$ 及 Q 与 $\overline{Q}$ 的角色，我们得到$(\eta)=PQ$ 及$(1+\eta)=P^3$ 或 $\overline{P}^3$. 因而在$\mathscr{C}$中有$\langle P\rangle^3=\langle 1\rangle$且$\langle Q\rangle=\langle P\rangle^{-1}$. 理想类群是 3 阶循环群.

引理(10.19)的证明 这个引理对单位理想 R 成立. 我们将证明如果 P 是素理想则$[R:P]=$

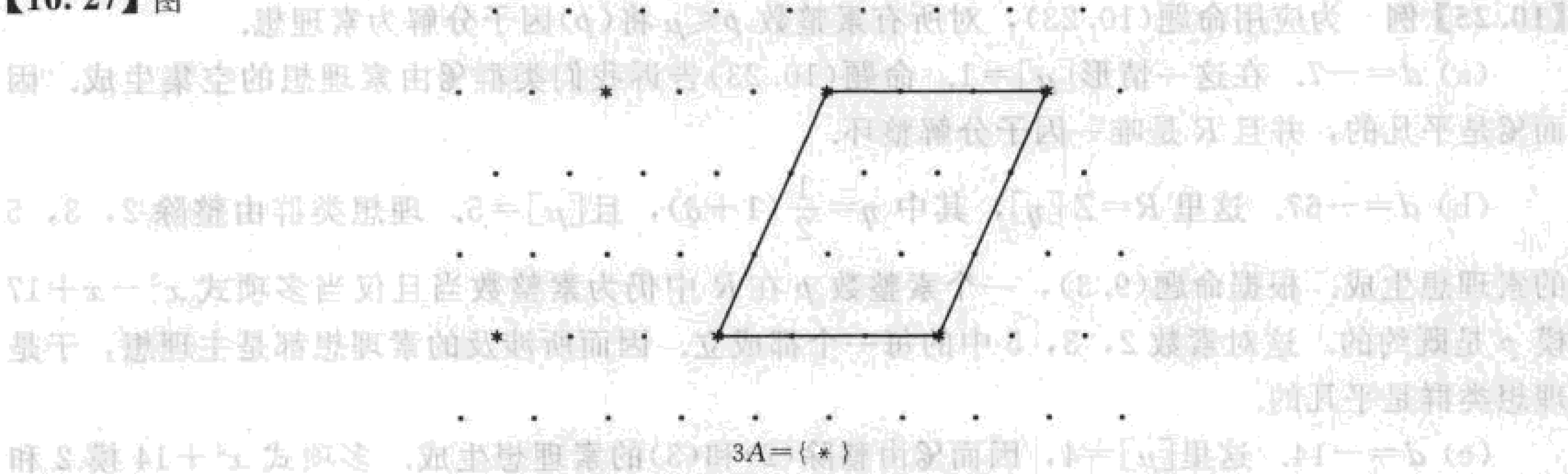
$N(P)$以及如果 P 是素理想且 A 是任意非零理想，则$[R:AP]=[R:A][R:P]$. 由此得到如果$[R:A]=N(A)$，则$[R:AP]=N(AP)$. 对一个理想的素因子分解的长度作归纳就可完成证明.

【10.26】引理 设 n 是普通整数，并设 A 是一个理想. 则

$$[R:nA]=n^2[R:A].$$

证明 我们知道 $R\supset A\supset nA$，因而由(10.14b)有$[R:nA]=[R:A][A:nA]$. 因此需要证明 432 $[A:nA]=n^2$. 这样 A 是一个格，nA 是由伸展一个因子 n 得到的子格：

【10.27】 图



显然，$[A:nA]=n^2$，这正是要证的. ■

我们回到引理(10.19)的证明. 对于理想 P 要考虑两种情形. 根据(9.1)，存在整素数 p 使得或者 $P=(p)$或者 $P\bar{P}=(p)$.

在第一种情形，$N(P)=p^2$，且 $AP=pA$. 可用引理(10.26)两次得到$[R:AP]=p^2[R:A]$及$[R:P]=p^2[R:R]=p^2$. 这样$[R:AP]=[R:A][R:P]$且$[R:P]=N(P)$，这正是要证的.

在第二种情形，$N(P)=p$. 考虑理想链 $A>AP>AP\bar{P}$. 由消去律(8.11a)这是一个理想的严格降链，因此

【10.28】
$$[R:A]<[R:AP]<[R:AP\bar{P}].$$

还有，由于 $P\bar{P}=(p)$，我们有 $AP\bar{P}=pA$. 因而可以再次应用引理(10.26)而得到$[R:AP\bar{P}]=p^2[R:A]$. 由于(10.28)中每个指标的确整除下一个，仅有的可能性为$[R:AP]=p[R:A]$. 把这一点用于 $A=R$ 的情形表明$[R:P]=p=N(P)$. 因而我们又得到$[R:AP]=[R:A][R:P]$及$[R:P]=N(P)$. 这就完成了证明. ■

第十一节 实二次域

本节我们简单地看一下实二次数域$\mathbb{Q}[\delta]$，其中 $\delta^2=d>0$. 我们将以域$\mathbb{Q}[\sqrt{2}]$作为一个例子. 这个域的整数环为

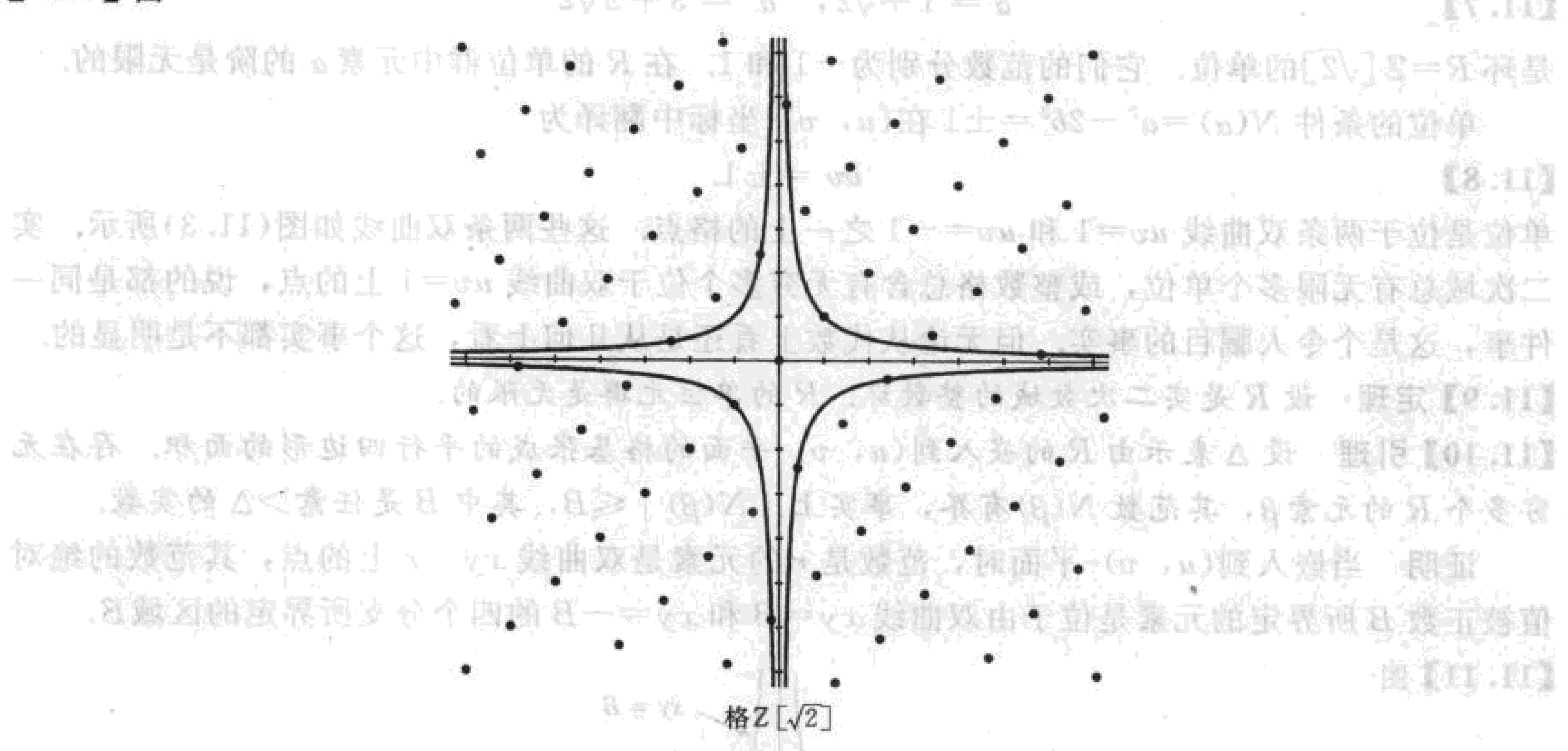
433 **【11.1】**
$$R=\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}.$$

由于$\mathbb{Q}[\sqrt{d}]$是实数的子域，整数环并没有作为子格嵌入复平面，但可以用系数(a,b)为坐标把 R 表示为一个格. R 作为格的稍微更为方便的表示是通过将代数整数 $a+b\sqrt{d}$ 与点(u,v)相伴，其中

【11.2】
$$u=a+b\sqrt{d},\quad v=a-b\sqrt{d}.$$

$d=2$ 时得到的格图示如下：

【11.3】图



格 $\mathbb{Z}[\sqrt{2}]$

由于 (u, v)-坐标与 (a, b)-坐标通过线性变换(11.2)联系起来，两种图示 R 的方法没有本质的区别．但由于变换不是正交的，在两个表示中格的形状是不同的．

回顾域 $\mathbb{Q}[\sqrt{d}]$ 同构于抽象构造的域

【11.4】 $$F=\mathbb{Q}[x]/(x^2-d).$$

我们用 F 代替 $\mathbb{Q}[\sqrt{d}]$ 而用 δ 表示 x 在 F 中的剩余．于是这个元素 δ 是 d 的一个抽象的平方根而不仅仅是正实平方根．这样坐标 u，v 代表抽象给定的域 F 嵌入实数的两个方法；即 u 使得 $\delta \rightsquigarrow \sqrt{d}$ 而 v 使得 $\delta \rightsquigarrow -\sqrt{d}$.

对 $\alpha=a+b\delta\in\mathbb{Q}[\delta]$，我们用 α' 表其"共轭"元素 $a-b\delta$．与虚二次情形(7.1)类似，α 的范数定义为

【11.5】 $$N(\alpha)=\alpha\alpha'=a^2-db^2.$$

如果 α 是代数整数，则 $N(\alpha)$ 是整数，但不一定为正的，而且

【11.6】 $$N(\alpha\beta)=\alpha\beta\alpha'\beta'=N(\alpha)N(\beta).$$

有了这样定义的范数，虚二次域中理想的唯一因子分解为素理想的证明就可以搬过来了．

实和虚二次域之间有两个值得注意的差别．第一个是对实二次域，同一类理想按(11.2)作为格嵌入 (u, v)-平面时不是相似的几何图形．特别地，主理想不一定相似于格 R．理由很简单：用元素 $\alpha=a+b\delta$ 乘使得 u-坐标伸缩 $a+b\sqrt{d}$ 倍而 v-坐标伸缩另一个倍数 $a-b\sqrt{d}$．这个事实使几何稍为复杂一些，而这也是先讨论虚二次情形的原因．它并没有从本质上改变我们的理论：类数仍是有限的．

第二个差别更重要一些．这就是在实二次域的整数环中有无限多个单位．由于代数整数的范数 $N(\alpha)$ 是一个通常的整数，像前面一样，一个单位必有范数 ±1[见(7.3)]，且若 $N(\alpha)=$

434

$\alpha\alpha'=\pm1$，则$\pm\alpha'$是α的逆，因而α为单位．例如，

【11.7】 $$\alpha=1+\sqrt{2},\quad \alpha^2=3+2\sqrt{2}$$

是环$R=\mathbb{Z}[\sqrt{2}]$的单位．它们的范数分别为-1和1．在R的单位群中元素α的阶是无限的．

单位的条件$N(\alpha)=a^2-2b^2=\pm1$在$(u,\ v)$-坐标中翻译为

【11.8】 $$uv=\pm1.$$

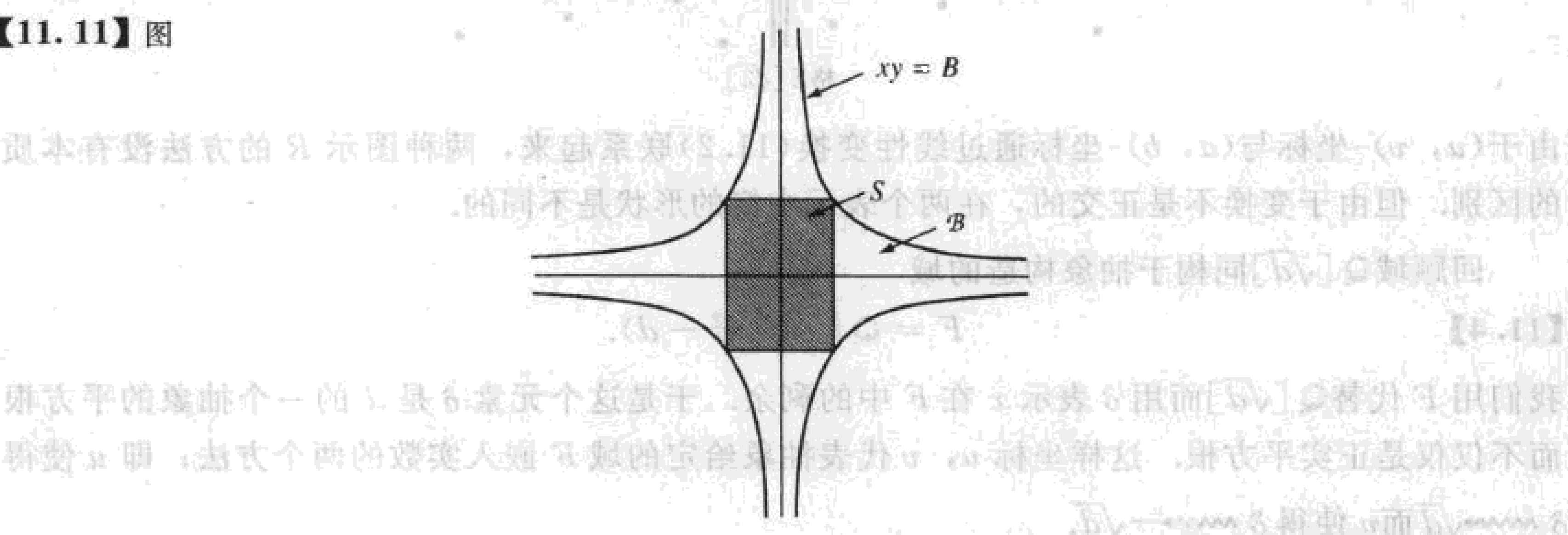
单位是位于两条双曲线$uv=1$和$uv=-1$之一上的格点．这些两条双曲线如图(11.3)所示．实二次域总有无限多个单位，或整数格总含有无穷多个位于双曲线$uv=1$上的点，说的都是同一件事，这是个令人瞩目的事实．但无论从代数上看还是从几何上看，这个事实都不是明显的．

【11.9】定理 设R是实二次数域的整数环．R的单位元群是无限的．

【11.10】引理 设Δ表示由R的嵌入到$(u,\ v)$-平面的格基张成的平行四边形的面积．存在无穷多个R的元素β，其范数$N(\beta)$有界，事实上$|N(\beta)|\leqslant B$，其中B是任意$>\Delta$的实数．

435 **证明** 当嵌入到$(u,\ v)$-平面时，范数是r的元素是双曲线$xy=r$上的点，其范数的绝对值被正数B所界定的元素是位于由双曲线$xy=B$和$xy=-B$的四个分支所界定的区域$\mathcal{B}$．

【11.11】图



选择任意一个正实数u_0．则顶点为$(\pm u_0,\ \pm B/u_0)$的长方形S完全属于区域$\mathcal{B}$，这个长方形的面积为$4B$．因而如果$B>\Delta$，则闵可夫斯基引理保证在S中存在一个非零格点α．这个点的范数由B界定．这对所有u_0都成立，且如果u_0非常大，则长方形S非常窄．另一方面，在u_0-轴上没有格点，因为在R中没有范数为零的非零元素．因而没有一个特定的格点能包含在所有长方形S中．由此得到在$\mathcal{B}$中存在无穷多个格点． ■

由于在区间$-B\leqslant r\leqslant B$中只有有限多个整数r，引理(11.10)蕴涵下面的推论：

【11.12】推论 存在整数r，使得R中存在无限多个具有范数r的元素．

设r是一个整数．如果在R中r整除$\beta_1-\beta_2$，则称R的两个元素$\beta_i=m_i+n_i\delta$模r同余．如果$d\equiv2$或3(模4)，这正好表明$m_1\equiv m_2$且$n_1\equiv n_2$(模r)．

【11.13】引理 设β_1，β_2是R的具有同样范数r的元素，且它们模r同余．则β_1/β_2是R的单位．

证明 只需证明β_1/β_2属于R即可，因为同样的论证将表明$\beta_2/\beta_1\in R$，因此β_1/β_2是一个单位．设$\beta_i'=m_i-n_i\delta$是β_i的共轭．则$\beta_1/\beta_2=\beta_1\beta_2'/\beta_2\beta_2'=\beta_1\beta_2'/r$．但$\beta_2'\equiv\beta_1'$(模$r$)，因而

436 $\beta_1\beta_2'\equiv\beta_1\beta_1'\equiv r$(模$r$)．因而$r$整除$\beta_1\beta_2'$，这表明$\beta_1/\beta_2\in R$，引理得证． ■

定理(11.9)的证明 选择r使得有无限多个元素$\beta=m+n\delta$的范数为r. 我们将这些元素的集合按照模r的同余类作划分. 由于有有限多个同余类，因此存在一个含有无限多个元素的类. 这些元素中任意两个之比都是一个单位. ■

第十二节 一些丢番图方程

丢番图方程是整系数多项式方程，要在整数中对它们进行求解. 最著名的是费马方程

【12.1】
$$x^n+y^n=z^n.$$

费马"最后定理"断言如果$n\geqslant 3$，那么除了其中一个变量为零的平凡解之外，没有整数解x，y，z. 费马在一本书的边上写下这个定理，并说书边太小写不下他的证明. 虽然已验证该定理对所有$n<10^5$成立，但今天仍不知道其证明[⊖]. 另外，法尔廷斯(Faltings)1983年证明的一个定理可应用于这个方程及许多其他方程，它指出对任意给定值n只有有限的整数解.

本节包含一些可用虚二次域的算术来求解的丢番图方程的例子. 它们在这里只是例子. 有兴趣的读者应阅读数论专著来了解对它更为系统的讨论.

我们有两个方法可用，即二次数域的算术和同余，并且两个方法都会用到.

【12.2】例 求使方程

$$x^2+y^2=n$$

有整数解的整数n.

这里的问题是求可以写成两个整数的平方和的整数n，或等价地，求使得在圆$x^2+y^2=n$上有整数坐标的点的整数n. 定理(5.1)告诉我们当p是素数时，方程$x^2+y^2=p$有整数解当且仅当$p=2$或$p\equiv 1$(模4). 不难将这个结果拓广到任意整数. 为此，我们将平方和a^2+b^2解释为高斯整数$\alpha=a+bi$的范数$\alpha\bar{\alpha}$. 于是问题变为确定哪些整数是高斯整数的范数. 如果一个高斯整数α因数分解为高斯素数，设$\alpha=\pi_1\cdots\pi_k$，则其范数亦有分解：$N(\alpha)=N(\pi_1)\cdots N(\pi_k)$. 这样如果$n$是高斯整数的范数，则它是高斯素数的范数的乘积，反之亦然. 高斯素数的范数是素数$p\equiv 1$(模4)，素数$p\equiv 3$(模4)的平方以及素数2. 这样我们有下列定理： 437

【12.3】定理 *方程$x^2+y^2=n$有整数解当且仅当在n的因数分解中每个模4与3同余的素数p有偶数次指数.*

【12.4】例 确定方程

$$y^2+13=x^3$$

的整数解.

对方程左边作因数分解，得到

$$(y+\delta)(y-\delta)=x^3,$$

其中$\delta=\sqrt{-13}$. 整数环$R=\mathbb{Z}[\delta]$不是唯一因子分解整环，因而我们用理想的因子分解来分析这个方程.

⊖ 译者注：该定理在1994年最终由英国数学家怀尔斯给出了完全的证明.

【12.5】引理 设 a，b 是整数，并设 R 是任意包含$\mathbb{Z}$作为其子环的环. 如果 a 和 b 包含在 R 的一个公共真理想 A 中，则它们在$\mathbb{Z}$中有一个公共素因数.

证明 用反证法. 如果 a，b 在$\mathbb{Z}$中没有公共素因数，则可以记 $1=ra+sb$，r，$s\in\mathbb{Z}$. 这个等式表明如果 a，b 属于 R 的一个理想 A，则亦有 $1\in A$. 因而 A 不是真理想. ■

【12.6】引理 设 x，y 是方程(12.4)的整数解. 在 R 中两个元素 $y+\delta$ 与 $y-\delta$ 没有公共的素理想因子.

证明 设 P 是包含 $y+\delta$ 和 $y-\delta$ 的素理想. 则 $2y\in P$ 并且 $2\delta\in P$. 由于 P 是素理想，因此或者$2\in P$,否则 $y\in P$ 且 $\delta\in P$.

在第一种情形，根据引理(12.5)，2 与 y^2+13 不是互素的整数，而由于 2 是素数，因此它在$\mathbb{Z}$中整除 y^2+13. 这表明 2 整除 x 且 8 整除 $y^2+13=x^3$. 因而 y 必为奇数. 于是 $y^2\equiv1$(模 4)；因此 $y^2+13\equiv2$(模 4). 这与 $x^3\equiv0$(模 8)矛盾.

假设 y，$\delta\in P$. 则 $13\in P$，因此 13 与 y 在$\mathbb{Z}$中不会互素，即 13 整除 y. 因而有 13 整除 x，以模 13^2 来看方程 $y^2+13=x^3$，我们得到 $13\equiv0$(模 13^2)，这是个矛盾. 因而得到 $y+\delta$ 与 $y-\delta$ 在 R 中是互素的. ■

现将方程$(y+\delta)(y-\delta)=(x)^3$ 看作 R 中主理想的等式，将右边因子分解为素理想，比如

$$(y+\delta)(y-\delta)=(P_1\cdots P_s)^3.$$

右边有立方，左边的两个理想没有公共素因子. 由此得到这两个理想的每一个也都是立方，设有理想 A 使得$(y+\delta)=A^3$ 而$(y-\delta)=\overline{A}^3$. 查一下理想类表，我们发现 R 的理想类群是 2 阶循环群. 因而 A 与 A^3 的理想类相等. 由于 A^3 是主理想，因而 A 也是，设有整数 u，v 使得 $A=(u+v\delta)$. 我们很幸运. 由于 R 的单位是±1，$(u+v\delta)^3=\pm(y+\delta)$. 必要时改变符号，可设 $(u+v\delta)^3=(y+\delta)$.

438

现在通过研究方程 $y+\delta=(u+v\delta)^3$ 来完成我们的讨论. 展开右边得

$$y+\delta=(u^3-39uv^2)+(3u^2v-13v^3)\delta.$$

因而 $y=u^3-39uv^2$ 而 $1=(3u^2-13v^2)v$. 第二个等式蕴涵 $v=\pm1$ 及 $3u^2-13=\pm1$. 只可能是 $u=\pm2$ 而 $v=-1$. 于是 $y=\pm70$ 而 $x=(u+v\delta)(u-v\delta)=17$. 这些值的确是解，因而方程 $y^2+13=x^3$ 的整数解是 $x=17$ 和 $y=\pm70$.

【12.7】例 求素整数 p 使得

$$x^2+5y^2=p$$

有整数解.

设 $\delta=\sqrt{-5}$，并设 $R=\mathbb{Z}[\delta]$. 我们知道主理想(p)在 R 中分裂当且仅当同余式 $x^2\equiv-5$(模 p)有整数解(9.3a). 如果$(p)=P\overline{P}$ 且如果 P 是主理想，比如设 $P=(a+b\delta)$，则$(p)=(a+b\delta)(a-b\delta)=(a^2+5b^2)$. 由于 R 中仅有的单位是±1，因而 $a^2+5b^2=\pm p$，且由于 a^2+5b^2 为正，因此 $a^2+5b^2=p$.

遗憾的是 R 不是主理想整环. 因而很有可能$(p)=P\overline{P}$ 但 P 不是主理想. 为进一步分析这种情形，我们用 R 中恰好有两个理想类这一事实. 主理想构成一类，而另一类由任一非主理想代表. 理想 $A=(2,\ 1+\delta)$是一个非主理想，并回顾对这个理想有 $A^2=A\overline{A}=(2)$. 现在由于

理想类群是 2 阶循环群，因此同一类中任意两个理想之积是主理想. 假设$(p)=P\overline{P}$且P不是主理想. 则AP是主理想，可设$AP=(a+b\delta)$. 则$(a+b\delta)(a-b\delta)=AP\,\overline{AP}=(2p)$. 我们得到$a^2+5b^2=2p$.

【12.8】引理 *设 p 是奇素数. 同余式 $x^2\equiv-5$(模 p)有解当且仅当两个方程 $x^2+5y^2=p$ 或 $x^2+5y^2=2p$ 之一有整数解.*

证明 如果同余式有解，则$(p)=P\overline{P}$，且两种情形如上面一样根据P是否为主理想确定. 反之，如果$x^2+5y^2=p$，则(p)在R中分裂，我们可以应用(9.3a). 如果$x^2+5y^2=2p$，则$(a+b\delta)(a-b\delta)=(2p)=A\overline{A}(p)$. 由理想的唯一因子分解可得$(p)$亦分裂，因而又可应用(9.3a). ■

该引理并没解决我们原来的问题，但已有了进展. 在大多数这样的情形中无法完成我们的分析. 但这里我们又很幸运，更应该说选择这个例子是因为它有完整的解：可以通过同余把这两种情形区别开来. 如果$a^2+5b^2=p$，则两个整数a，b之一为奇而另一为偶. 我们计算模 4 的同余，得到$a^2+5b^2\equiv1$(模 4). 因此在此情形有$p\equiv1$(模 4). 如果$a^2+5b^2=2p$，我们计算模 8 的同余. 由于$p\equiv1$或 3(模 4)，我们知道$2p\equiv2$或 6(模 8). 任意数的平方与 0，1 或 4(模 8)同余，这表明a^2+5b^2不能与 2(模 8)同余. 这样在此情形有$p\equiv3$(模 4). 因而我们证明了下面的引理： [439]

【12.9】引理 *设 p 是奇素数. 假设同余式 $x^2\equiv-5$(模 p)有一个解. 则当 $p\equiv1$(模 4)时，$x^2+5y^2=p$ 有整数解，而当 $p\equiv3$(模 4)时 $x^2+5y^2=2p$ 有整数解.*

最后还剩下刻画使同余式$x^2\equiv-5$模p有解的奇素数p的问题. 这由令人惊讶的*二次互反律*实现，它断言$x^2\equiv5$(模p)有解当且仅当$x^2\equiv p$(模 5)有解！而第二个同余式有解当且仅当$p\equiv\pm1$(模 5). 将其与前面的引理以及-1是模 5 的平方数这一事实结合起来，我们得到：

【12.10】定理 *设 p 是奇素数. 方程 $x^2+5y^2=p$ 有整数解当且仅当 $p\equiv1$(模 4)并且 $p\equiv\pm1$(模 5).*

> 对于经过努力仍未解决的问题，
> 如果没有大量卓有成效的创造，
> 我们就看不到问题的本质所在.
>
> *Karl Friedrich Gauss*

练　习

第一节　整数和多项式的因子分解

1. 设a，b是其和为素数p的正整数. 证明其最大公因数为 1.
2. 定义n个整数的集合的最大公因数，并证明其存在性.
3. 证明如果d是a_1，…，a_n的最大公因数，则a_1/d，…，a_n/d的最大公因数是 1.
4. (a) 证明如果n是正整数，且不是一个整数的平方，则$\sqrt{n}$不是有理数.
   (b) 对n次根证明类似的结论.
5. (a) 设a，b是整数且$a\neq0$，记$b=aq+r$，其中$0\leqslant r<|a|$. 证明两个最大公因数(a,b)与(a,r)相等.
   (b) 描述一个基于(a)的计算最大公因数的算法. [440]

(c) 用你的算法计算下面的最大公因数：

a) 1456，235　b) 123456789，135792468．

6. 求下列多项式的最大公因式：x^3-6x^2+x+4，x^5-6x+1.

7. 证明：如果系数属于域 F 的两个多项式 f，g 在域 F 中分解为线性因式，则它们的最大公因式是它们的公共线性因式的积.

8. 在$\mathbb{F}_p[x]$中将下列多项式分解为既约因式.

(a) x^3+x+1，$p=2$　(b) x^2-3x-3，$p=5$　(c) x^2+1，$p=7$

9. 欧几里得用下面的方法证明了存在无穷多个素整数：如果 p_1，…，p_k 是素数，则 $n=(p_1\cdots p_n)+1$ 的任意素因子必不同于所有 p_i.

(a) 改写这个论证以证明对任意域 F，在 $F[x]$中存在无穷多个首一既约多项式.

(b) 解释为什么这个论证对于形式幂级数环 $F[[x]]$不成立.

10. 整数的部分分数：

(a) 将分数 $r=7/24$ 写为 $r=a/8+b/3$ 的形式.

(b) 证明如果 $n=uv$，其中 u，v 互素，则每个分数 $r=m/n$ 可以写为 $r=a/u+b/v$ 的形式.

(c) 设 $n=n_1n_2\cdots n_k$ 是一个整数分解为不同的素数幂的因数分解：$n_i=p_i^{e_i}$. 证明每个分数 $r=m/n$ 可以写为 $r=m_1/n_1+m_2/n_2+\cdots+m_k/n_k$ 的形式.

11. 中国剩余定理：

(a) 设 n，m 为互素的整数，并设 a，b 是任意整数. 证明存在整数 x 同时是同余式 $x\equiv a$(模 m)及 $x\equiv b$(模 n)的解.

(b) 求这两个同余式所有的解.

12. 求下列同余式的公共解.

(a) $x\equiv3$(模 15)，$x\equiv5$(模 8)，$x\equiv2$(模 7)

(b) $x\equiv13$(模 43)，$x\equiv7$(模 71)

13. 多项式的部分分式：

(a) 证明$\mathbb{C}[x]$的每个有理函数可以写为一个多项式与一个形如 $1/(x-a)^i$ 的函数的线性组合的和.

(b) 求$\mathbb{C}(x)$作为$\mathbb{C}$的向量空间的一个基.

*14. 设 F 是$\mathbb{C}$的一个子域，设 $f\in F[x]$是一个既约多项式. 证明 f 在$\mathbb{C}$中没有重根.

15. 证明两个多项式 f 和 g 在$\mathbb{Q}[x]$中的最大公因式也是它们在$\mathbb{C}[x]$中的最大公因式.

16. 设 a，b 为互素的整数. 证明存在整数 m，n 使得 $a^m+b^n\equiv1$(模 ab).

第二节　唯一因子分解整环、主理想整环与欧几里得整环

1. 证明或推翻下列说法：

(a) 二元多项式环$\mathbb{R}[x, y]$是欧几里得整环.

441

(b) 环$\mathbb{Z}[x]$是主理想整环.

2. 证明下列环是欧几里得整环.

(a) $\mathbb{Z}[\zeta]$，$\zeta=e^{2\pi i/3}$　(b) $\mathbb{Z}[\sqrt{-2}]$

3. 举例说明在欧几里得整环中带余除法不一定是唯一的.

4. 设 m，n 为两个整数. 证明它们在$\mathbb{Z}$中的最大公因数与它们在$\mathbb{Z}[i]$中的最大公因数相等.

5. 证明整环中每一个素元都是既约元.

6. 证明命题(2.8)，即证明存在因子分解的整环 R 是唯一因子分解整环当且仅当每个既约元都是素元.

7. 证明在一个主理想整环 R 中，每一对不全为零的元素 a，b 都有具有下列性质的最大公因子 d：

(i) 存在 r，$s\in R$ 使得 $d=ar+bs$；

(ii) d 整除 a 和 b；

(iii) 如果 $e\in R$ 整除 a 和 b，它亦整除 d.

而且，d 在单位因子下唯一确定.

8. 在$\mathbb{Z}[\mathrm{i}]$中求$(11+7\mathrm{i},\ 18-\mathrm{i})$的最大公因数.

9. (a) 证明在环 $R=\mathbb{Z}[\sqrt{-5}]$中 2，3，$1\pm\sqrt{-5}$为既约元并且这个环的单位元为± 1.

(b) 证明在这个环中因子分解的存在性成立.

10. 证明形式实幂级数环$\mathbb{R}[[t]]$是唯一因子分解整环.

11. (a) 证明如果 R 是整环，则两个元素 a，b 相伴当且仅当它们相差一个单位因子.

*(b) 举例说明当 R 不是整环时(a)不成立.

12. 设 R 是主理想整环.

(a) 证明存在两个不全为零的元素的*最小公倍子*$[a,\ b]=m$ 使得 a，b 整除 m，且如果 a，b 整除一个元素 $r\in R$,则 m 整除 r. 证明除了相差单位因子外 m 唯一.

(b) 用$(a,\ b)$记 a 与 b 的最大公因子. 证明$(a,\ b)[a,\ b]$与 ab 相伴.

13. 如果 a，b 是整数且在高斯整数环中 a 整除 b，则在$\mathbb{Z}$中 a 整除 b.

14. (a) 证明通过在多项式环上添加 x 的 2^k 次根 x_k 得到的环$R(2.4)$是多项式环 $F[x_k]$的并.

(b) 证明在 R 中不存在 x_1 分解成为既约因子的因子分解.

15. 一个因子分解 $a=b_1\cdots b_k$ 的*加细*是指通过因子分解项 b_i 得到的 a 的表达式. 设 R 是环(2.4). 证明同一个元素 $a\in R$ 的任意两个因子分解有其所有因子皆相伴的加细.

16. 设 R 是环 $F[u,\ v,\ y,\ x_1,\ x_2,\ x_3,\ \cdots]/(x_1y=uv,\ x_2^2=x_1,\ x_3^2=x_2,\ \cdots)$. 证明 u，v 是 R 的既约元而分解 uv 的过程不会终止.

17. 证明命题(2.9)及推论(2.10).

18. 证明命题(2.11).

19. 证明(2.22)的因子分解在$\mathbb{Z}[\mathrm{i}]$中是素分解.

20. 唯一因子分解的讨论仅涉及环 R 上的乘法法则，因而应当可能拓展这个定义. 设 S 是一个交换半群，也就是一个具有满足交换律和结合律的合成法则且有单位元的集合. 假设在 S 中消去律成立：如果 $ab=ac$，则 $b=c$. 给出适当的定义使命题(2.8)能拓广到这种情形.

*21. 给定$\mathbb{Z}^2$ 的元素 v_1，…，v_n，我们可以定义半群 S 为$(v_1,\ \cdots,\ v_n)$的具有非负整系数的线性组合的集合，合成法则为*加法*. 确定这样的半群中哪些具有唯一因子分解.

第三节 高斯引理

1. 设 a，b 是域 F 的元素，且 $a\neq 0$. 证明多项式 $f(x)\in F[x]$既约当且仅当 $f(ax+b)$既约.

2. 设 $F=\mathbb{C}[x]$，并设 f，$g\in\mathbb{C}[x,\ y]$. 证明如果 f 和 g 在 $F[y]$中有公因式，则它们在$\mathbb{C}[x,\ y]$中也有公因式.

3. 设 f 是$\mathbb{C}[x,\ y]$中的一个既约多项式，并设 g 是另一个多项式. 证明如果 g 在$\mathbb{C}^2$ 中的零点的簇包含 f 的零点的簇，则 f 整除 g.

4. 证明两个整多项式在$\mathbb{Q}[x]$中互素当且仅当它们在$\mathbb{Z}[x]$中生成的理想含有一个整数.

5. 用下面的方法不模 p 约化而证明高斯引理：设 a_i 是 f 的不为 p 整除的最低次系数. 因而如果 $v<i$，则 p 整除 a_v，但 p 不整除 a_i. 类似地，设 b_j 是 g 的不为 p 整除的最低次系数. 证明 h 的 $i+j$ 次系数不为 p 整除.

6. 对欧几里得整环叙述并证明高斯引理.

7. 证明一个整多项式是本原的当且仅当它不包含于任意映射(3.2)的核.

442

8. 证明 $\det\begin{bmatrix} x & y \\ z & w \end{bmatrix}$在多项式环$\mathbb{C}[x, y, z, w]$中是既约的.

9. 证明使 $x \rightsquigarrow 1+\sqrt{2}$的同态$\mathbb{Z}[x] \longrightarrow \mathbb{R}$ 的核是主理想，并求出这个理想的生成元.

10. (a) 考虑由 $f(x, y) \rightsquigarrow f(t^2, t^3)$定义的映射 ψ: $\mathbb{C}[x, y] \longrightarrow \mathbb{C}[t]$. 证明其核是一个主理想，其象是使 $p'(0)=0$ 的多项式 $p(t)$的集合.

    (b) 考虑由 $f(x, y) \rightsquigarrow (t^2-t, t^3-t^2)$定义的映射 φ:$\mathbb{C}[x, y] \longrightarrow \mathbb{C}[t]$. 证明 $\ker\varphi$ 是一个主理想，其象是使 $p(0)=p(1)$的多项式 $p(t)$的集合. 用$\mathbb{C}^2$ 中簇$\{f=0\}$的几何给出一个直观的解释.

第四节 多项式的具体分解

1. 证明下列多项式在$\mathbb{Q}[x]$中既约.

   (a) $x^2+27x+213$ (b) $x^3+6x+12$ (c) $8x^3-6x+1$ (d) x^3+6x^2+7 (e) x^5-3x^4+3

2. 在$\mathbb{Q}[x]$和$\mathbb{F}_2[x]$中将 x^5+5x+5 分解成既约因式.

443

3. 在$\mathbb{F}_p[x]$中将 x^3+x+1 分解因式，其中 $p=2, 3, 5$.

4. 在$\mathbb{Q}[x]$中将 x^4+x^2+1 分解成既约因式.

5. 假设形如 x^4+bx^2+c 的多项式是$\mathbb{Q}[x]$中两个二次因式的积. 对这两个因式的系数会有什么结论?

6. 证明下列多项式是既约的.

   (a) x^2+x+1 在域$\mathbb{F}_2$ 上 (b) x^2+1 在域$\mathbb{F}_7$ 上 (c) x^3-9 在域$\mathbb{F}_{31}$上

7. 在$\mathbb{Q}[x]$中分解下列多项式为既约因式的乘积.

   (a) x^3-3x-2 (b) x^3-3x+2 (c) $x^9-6x^6+9x^3-3$

8. 设 p 是素整数. 证明多项式 x^n-p 在$\mathbb{Q}[x]$中既约.

9. 借助于模 2 约化，在$\mathbb{Q}[x]$中分解下列多项式.

   (a) $x^2+2345x+125$ (b) $x^3+5x^2+10x+5$ (c) x^3+2x^2+3x+1

   (d) $x^4+2x^3+2x^2+2x+2$ (e) $x^4+2x^3+3x^2+2x+1$

   (f) $x^4+2x^3+x^2+2x+1$ (g) $x^5+x^4-4x^3+2x^2+4x+1$

10. 设 p 是素整数，并设 $f\in\mathbb{Z}[x]$是 $2n+1$ 次的多项式，如 $f(x)=a_{2n+1}x^{2n+1}+\cdots+a_1x+a_0$. 假设 $a_{2n+1}\not\equiv 0$(模 p)，$a_0, a_1\cdots, a_n\equiv 0$(模 p^2)，$a_{n+1}, \cdots, a_{2n}\equiv 0$(模 p)，$a_0\not\equiv 0$(模 p^3). 证明 f 在$\mathbb{Q}[x]$中既约.

11. 设 p 是素数，并设 $A\neq I$ 是一个 $n\times n$ 整数矩阵满足 $A^p=I$ 但 $A\neq I$. 证明 $n\geqslant p-1$.

12. 确定$\mathbb{F}_3$ 上的 3 次首一既约多项式.

13. 确定$\mathbb{F}_5$ 上的 2 次首一既约多项式.

14. 拉格朗日插值公式:

    (a) 设 $x_0, \cdots, x_d$ 是不同的复数. 求一个在 $x_1, \cdots, x_n$ 处为零并使 $p(x_0)=1$ 的 n 次多项式 $p(x)$.

    (b) 设 $x_0, \cdots, x_d, y_0, \cdots, y_d$ 是复数，并假设 x_i 互不相同. 存在唯一一个$\leqslant d$ 次的多项式 $g(x)\in\mathbb{C}[x]$，使得对每个 $i=0, \cdots, d$ 有 $g(x_i)=y_i$. 通过用 x_i, y_i 具体确定多项式 g 来证明这个结果.

*15. 利用拉格朗日插值公式给出一个在有限步内找到一个整多项式的所有整多项式因式的方法.

16. 设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是首一整系数多项式，并设 $r\in\mathbb{Q}$ 是 $f(x)$的一个有理根. 证明 r 是个整数.

17. 用待定系数法，即通过研究等式$(ax+by+c)(a'x+b'y+c')=x^2+y^2-1$(其中 a, b, c, a', b', c'是未知量)来证明多项式 x^2+y^2-1 既约.

第五节 高斯整数环中的素元

1. 证明每个高斯素数只整除恰好一个整素数.

2. 在$\mathbb{Z}[i]$中将 30 因数分解为素数乘积.
3. 将下列各数分解为高斯素数乘积.
   (a) $1-3i$ (b) 10 (c) $6+9i$
4. 作一个清楚的图，表出在适当大小范围内的高斯整数环的素数.
5. 设π为高斯素数. 证明π与$\bar{\pi}$相伴当且仅当π与一个整素数相伴或者$\pi\bar{\pi}=2$.

444

6. 设R是环$\mathbb{Z}[\sqrt{3}]$. 证明素整数p是R中的素元素当且仅当多项式x^2-3在$\mathbb{F}_p[x]$中既约.
7. 在下面每一情形描述剩余环$\mathbb{Z}[i]/(p)$.
   (a) $p=2$ (b) $p\equiv1$(模 4) (c) $p\equiv3$(模 4)

*8. 设$R=\mathbb{Z}[\zeta]$，其中$\zeta=\frac{1}{2}(-1+\sqrt{-3})$是 1 的一个复立方根. 设$p$是一个不等于 3 的整素数. 修改定理(5.1)的证明，以证明下列断言.
   (a) 多项式x^2+x+1在$\mathbb{F}_p$中有一个根当且仅当$p\equiv1$(模 3).
   (b) (p)是R的素理想当且仅当$p\equiv-1$(模 3).
   (c) p在R中可以分解当且仅当存在整数a，b使得p可写为$p=a^2+ab+b^2$的形式.
   (d) 作图表出R中绝对值$\leqslant10$的素数.

第六节 代数整数

1. $\frac{1}{2}(1+\sqrt{3})$是代数整数吗？
2. 设α是在$\mathbb{Z}$上的首一既约多项式为$x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$的代数整数，并设$R=\mathbb{Z}[\alpha]$. 证明$\alpha$是$R$的单位当且仅当$a_0=\pm1$.
3. 设d，d'是不同的无平方整数. 证明$\mathbb{Q}[\sqrt{d}]$与$\mathbb{Q}[\sqrt{d'}]$是$\mathbb{C}$中不同的子域.
4. 证明在虚二次数域的整数环中因数分解的存在性成立.
5. 设α是 10 的实立方根，并设$\beta=a+b\alpha+c\alpha^2$，其中$a$，$b$，$c\in\mathbb{Q}$. 则$\beta$是一个首一三次多项式$f(x)\in\mathbb{Q}[x]$的根. α在$\mathbb{Q}$上的既约多项式是x^3-10，它的三个根为α，$\alpha'=\zeta\alpha$和$\alpha''=\zeta^2\alpha$，其中$\zeta=e^{2\pi i/3}$. f的三个根是β，$\beta'=a+b\zeta\alpha+c\zeta^2\alpha^2$和$\beta''=a+b\zeta^2\alpha+c\zeta\alpha^2$，因而$f(x)=(x-\beta)(x-\beta')(x-\beta'')$.
   (a) 展开这个积来确定f. 含有α和α^2的项会被消去，因而不必计算.
   (b) 确定哪个元素β是代数整数.
6. 证明命题(6.17).
7. 证明在虚二次域中整数环是具有在复平面上成为格这一性质的$\mathbb{C}$的极大子环.
8. (a) 设$S=\mathbb{Z}[\alpha]$，其中α是二次首一多项式的一个复根. 证明S是复平面上的一个格.
   (b) 证明其逆：$\mathbb{C}$中成为格的子环S具有(a)中给出的形式.
9. 设R是域$\mathbb{Q}[\sqrt{d}]$中的整数环.
   (a) 求使$R=\mathbb{Z}[\alpha]$的元素$\alpha\in R$.
   (b) 证明如果$R=\mathbb{Z}[\alpha]$且若α是$\mathbb{Q}$上多项式x^2+bx+c的根，则判别式b^2-4c为D(6.18).

第七节 虚二次域中的因数分解

1. 用算术证明命题(7.3).
2. 证明元素 2，3，$1+\sqrt{-5}$，$1-\sqrt{-5}$是环$\mathbb{Z}[\sqrt{-5}]$的既约元.

445

3. 设$d=-5$. 确定给定向量的整线性组合的格是否是一个理想.
   (a) $(5, 1+\delta)$ (b) $(7, 1+\delta)$ (c) $(4-2\delta, 2+2\delta, 6+4\delta)$
4. 设A是虚二次域中整数环R的一个理想. 证明存在A的格基，其中一个元素是正整数.

5. 设 $R=\mathbb{Z}[\sqrt{-5}]$. 证明由 $(3, 1+\sqrt{-5})$ 张成的格是 R 的理想，求它的具有极小绝对值的非零元，并验证这个理想具有(7.9)中情形 2 的形式.

6. 用(7.9)的记号，证明如果 α 是 R 中使 $\frac{1}{2}(\alpha+\alpha\delta)$ 亦属于 R 的元素，则 $\left(\alpha, \frac{1}{2}(\alpha+\alpha\delta)\right)$ 是理想的一个格基.

7. 对下列每个环，用命题(7.9)的方法描述 R 中的理想. 作图表出每一情形格的形状.

   (a) $R=\mathbb{Z}[\sqrt{-3}]$ (b) $R=\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-3})\right]$ (c) $R=\mathbb{Z}[\sqrt{-6}]$

   (d) $R=\mathbb{Z}[\sqrt{-7}]$ (e) $R=\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-7})\right]$ (f) $R=\mathbb{Z}[\sqrt{-10}]$

8. 证明当 $d\equiv 2$(模 4)并且 $d<-2$ 时，R 不是唯一因子分解整环.

9. 设 $d\leqslant -3$. 证明在环 $\mathbb{Z}[\sqrt{d}]$ 中 2 不是素元，但 2 是这个环的既约元.

第八节 理想因子分解

1. 设 $R=\mathbb{Z}[\sqrt{-6}]$. 将理想(6)具体分解为素理想的乘积.

2. 设 $\delta=\sqrt{-3}$ 而 $R=\mathbb{Z}[\delta]$.（这不是虚二次数域 $\mathbb{Q}[\delta]$ 中的整数环.）设 A 是理想 $(2, 1+\delta)$. 证明 $A\overline{A}$ 不是主理想，因此主要引理对这个环不成立.

3. 设 $R=\mathbb{Z}[\sqrt{-5}]$. 确定 11 是否是 R 的既约元，以及(11)是否是 R 的素理想.

4. 设 $R=\mathbb{Z}[\sqrt{-6}]$. 求积理想 AB 的一个格基，其中 $A=(2, \delta)$ 而 $B=(3, \delta)$.

5. 证明 $A\supset A'$ 蕴涵 $AB\supset A'B$.

6. 在 $R=\mathbb{Z}[\delta]$ 中将主理想(14)具体分解为素理想的乘积，其中 $\delta=\sqrt{-5}$.

7. 设 P 是整环 R 的素理想，并假设在 R 中因子分解存在. 证明如果 $\alpha\in P$，则 α 的某个既约因子属于 P.

第九节 R 的素理想与素整数的关系

1. 在(a) $\mathbb{Q}[\sqrt{-14}]$ 和(b) $\mathbb{Q}[\sqrt{-23}]$ 的整数环中求 2 和 3 的素因子的格基.

2. 设 $d=-14$. 对下面每一个素数 p 确定 p 是否在 R 中分裂或分歧，如果是的话，确定 (p) 的素理想因子的格基：2，3，5，7，11，13.

3. (a) 假设素整数 p 在 R 中保持素性. 证明这时 $R/(p)$ 是有 p^2 个元素的一个域.

   446 (b) 证明若 p 在 R 中分裂，则 $R/(p)$ 同构于积环 $\mathbb{F}_p\times\mathbb{F}_p$.

4. 设 p 是在 R 中分裂的素数，如设 $(p)=P\overline{P}$，并设 $\alpha\in P$ 是不被 p 整除的任一元素. 证明作为理想 P 由 (p, α) 生成.

5. 证明命题(9.3b).

6. 如果 $d\equiv 2$ 或 3(模 4)，则由命题(9.3a)，如果 x^2-d 模 p 既约，则素整数 p 在 $\mathbb{Q}[\sqrt{d}]$ 的整数环中保持素性.

   (a) 当 $d\equiv 1$(模 4)而 $p\neq 2$ 时证明相同的结果.

   (b) 这一情形中 $p=2$ 时会发生什么？

7. 假设 $d\equiv 2$ 或 3(模 4). 证明素整数 p 在 R 中分歧当且仅当 $p=2$ 或 p 整除 d.

8. 当 d 模 4 与 1 同余时叙述并证明问题 7 的类似结论.

9. 设 p 是在 R 中分歧的整素数，比如设 $(p)=P^2$. 求 P 的一个具体的格基. 在什么情形下 P 是主理想？

10. 一个素整数可以具有 a^2+b^2d 的形式，其中 $a, b\in\mathbb{Z}$. 仔细讨论这是如何与 (p) 在 R 中的素因子分解联系起来的.

*11. 证明命题(9.1).

第十节 虚二次域的理想类

1. 证明理想 A 与 A' 相似当且仅当存在非零理想 C 使得 AC 和 $A'C$ 是主理想.
2. 通过研究圆上而不是任意中心对称凸集中的格点可以将推论(10.12)的估计改进为 $|\alpha|^2 \leqslant 2\Delta(L)/\sqrt{3}$. 推导出这个结果.
3. 设 $R=\mathbb{Z}[\delta]$，$\delta^2=-6$.
   (a) 证明格 $P=(2,\delta)$ 及 $Q=(3,\delta)$ 是 R 的素理想.
   (b) 在 R 中将主理想(6)具体分解为素理想.
   (c) 证明 P 和 Q 的理想类相等.
   (d) R 的闵可夫斯基上界是 $[\mu]=3$. 用这一事实确定 R 的理想类群.
4. 在以下每一情形，求理想类群并作图表出格的可能形状.
   (a) $d=-10$ (b) $d=-13$ (c) $d=-14$ (d) $d=-15$ (e) $d=-17$ (f) $d=-21$
5. 证明定理(7.7)所列的 d 的值有唯一因子分解.
6. 证明引理(10.13).
7. 由引理(10.13)推导出推论(10.14).
8. 验证表(10.24).

第十一节 实二次域

1. 设 $R=\mathbb{Z}[\delta]$，$\delta=\sqrt{2}$. 利用格嵌入(11.2)定义 R 上的大小函数：$\sigma(a+b\delta)=a^2-2b^2$. 证明这个大小函数使 R 成为欧几里得整环.
2. 设 R 是 $d\equiv 2$ 或 3(模 4)的实二次数域中的整数环. 根据(6.14)，R 具有形式 $\mathbb{Z}[x]/(x^2-d)$. 也可考虑 $R'=\mathbb{R}[x]/(x^2-d)$，它包含 R 为其子环.
   (a) 证明 R' 的元素以这样的方式与 $\mathbb{R}^2$ 的点一一对应：使得 R 的元素对应于格点.

447

   (b) 确定 R' 的单位群. 证明 R' 中由位于两条双曲线 $xy=\pm 1$ 上的点组成的子集 U' 构成单位群的一个子群.
   (c) 证明 R 的单位的群 U 是 U' 的离散子群，并证明属于第一象限的单位子群 U_0 是无限循环群.
   (d) 什么是单位群 U 的可能的结构?
3. 用 U_0 表示在嵌入(11.2)中的 R 的属于第一象限的单位群. 当(a) $d=3$，(b) $d=5$ 时求 U_0 的生成元.
4. 证明如果 d 是 >1 的平方数，则方程 $x^2-y^2d=1$ 除了 $x=\pm 1$，$y=0$ 没有其他解.
5. 对 $d=3$ 作适当大小范围的图展示双曲线及单位.

第十二节 一些丢番图方程

1. 求使 $x^2+5y^2=2p$ 有解的素数.
2. 用模 20 的同余表达定理(12.20)的断言.
3. 证明如果 $x^2\equiv -5$(模 p)有解，则在两个椭圆 $x^2+5y^2=p$ 和 $2x^2+2xy+3y^2=p$ 之一上有一个整点.
4. 确定关于整数 a，b，c 的条件，使得线性丢番图方程 $ax+by=c$ 有一个整数解，且如果它有解，求出所有的解.
5. 求素数 p 使得方程 $x^2+2y^2=p$ 有一个整数解.
6. 求素数 p 使得方程 $x^2+xy+y^2=p$ 有一个整数解.
7. 证明如果同余式 $x^2\equiv -10$(模 p)有解，则方程 $x^2+10y^2=p^2$ 有一个整数解. 并推广这个结论.
8. 求方程 $x^2+2=y^3$ 的所有整数解.
9. 解下列丢番图方程.
   (a) $y^2+10=x^3$ (b) $y^2+1=x^3$ (c) $y^2+2=x^3$

杂题

1. 证明存在无穷多个模 4 与 1 同余的素数.
2. 设 p_1, p_2, …, p_r 是前 r 个素数，通过研究整数 $p_1p_2\cdots p_r-1$ 的因子分解，证明存在无穷多个素数模 6 与 −1同余.
3. 证明存在无穷多个素数模 4 与 −1 同余.
4. (a) 确定二元多项式环$\mathbb{C}[x, y]$的素理想.
   (b) 证明环$\mathbb{C}[x, y]$中理想的唯一因子分解定理不成立.
5. 将一个整环中的元素的真因子分解与主理想的真因子分解联系起来. 利用这种联系，叙述并证明主理想整环中的理想的唯一因子分解定理.
6. 设 R 是整环，并设 I 是一个理想，它以两种方式写为不同的极大理想的积，比如设 $I=P_1\cdots P_r=Q_1\cdots Q_s$. 证明除了项的顺序，两个因子分解是一样的.

448

7. 设 R 是包含$\mathbb{Z}$为其子环的环. 证明如果整数 m, n 包含在 R 的一个真理想中，则它们有一个整公因数>1.

*8. (a) 设 θ 是群$\mathbb{R}^+/\mathbb{Z}^+$ 的一个元素. 用鸽笼原理[附录(1.6)]证明对每个整数 n 存在一个整数 $b\leqslant n$ 使得 $|b\theta|\leqslant\frac{1}{bn}$.
   (b) 证明对每个实数 r 及每个 $\varepsilon>0$，存在分数 m/n 使得 $|r-m/n|\leqslant\varepsilon/n$.
   (c) 通过证明对每个复数 α 及每个实数 $\varepsilon>0$，存在$\mathbb{Z}[i]$的一个元素，如 $\beta=(a+bi)/n$，其中 a, b, $n\in\mathbb{Z}$，使得 $|\alpha-\beta|\leqslant\varepsilon/n$. 将这个结果拓广到复数.
   (d) 设 ε 是一个正实数，对$\mathbb{Q}[i]$的每一个元素 $\beta=(a+bi)/n$，其中 a, b, $n\in\mathbb{Z}$，考虑以 β 为圆心半径为 ε/n 的圆盘. 证明这些圆盘的内部覆盖了复平面.
   (e) 拓广命题(7.9)的方法证明任意虚二次域的类数有限.

*9. (a) 设 R 是 $\cos t$ 和 $\sin t$ 的实系数多项式的函数环. 证明 $R\approx\mathbb{R}[x, y]/(x^2+y^2-1)$.
   (b) 证明 R 不是唯一因子分解整环.
   *(c) 证明$\mathbb{C}[x, y]/(x^2+y^2-1)$是主理想整环因而是唯一因子分解整环.

*10. 在欧几里得整环的定义中，假设大小函数 σ 的值域为非负整数的集合. 我们可将其推广到允许其值域为某些其他有序集. 考虑积环 $R=\mathbb{C}[x]\times\mathbb{C}[y]$. 证明可以定义一个大小函数 $R-\{0\}\longrightarrow S$，其中 S 是有序集 $\{0, 1, 2, 3, \cdots, \omega, \omega+1, \omega+2, \omega+3, \cdots\}$，使得带余除法成立.

*11. 设 $\varphi:\mathbb{C}[x, y]\longrightarrow\mathbb{C}[t]$为同态，比如由 $x\rightsquigarrow x(t)$, $y\rightsquigarrow y(t)$定义. 证明如果 $x(t)$, $y(t)$不同时为常数，则 $\ker\varphi$ 是一个非零主理想.

449

第十二章　模

敍聪明点！做推广！

Picayune Sentinel

第一节　模的定义

设 R 是交换环，一个 R-模 V 是一个带有记作 + 的合成法则的阿贝尔群与一个记作 r，$v \rightsquigarrow rv$ 的标量积 $R\times V \longrightarrow V$，满足下列公理：

【1.1】

$$\text{(i)}\quad 1v = v,$$
$$\text{(ii)}\quad (rs)v = r(sv),$$
$$\text{(iii)}\quad (r+s)v = rv + sv,$$
$$\text{(iv)}\quad r(v+v') = rv + sv',$$

对所有 r，$s\in R$ 和 v，$v'\in V$ 都成立．注意到这几条恰好是一个向量空间的公理．当 F 是域时，一个 F 模正好是一个 F-向量空间．因而模是向量空间到环上的自然推广．但环的元素不必可逆这一事实使得模更为复杂．

最明显的例子是 R-向量的模 R^n，即有 R 中元素的行向量和列向量的模．R-向量的合成法则与元素在一个域中的向量的合成法则是一样的：

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{bmatrix},\quad r\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} ra_1 \\ \vdots \\ ra_n \end{bmatrix}.$$

这样定义的模称为自由模．但当 R 不是域时，这些模不再是仅有的模．存在不同构于任意自由模的模，即使它们是由有限集合张成的．

在 R 是整数环 $\mathbb{Z}$ 的情形考察模的概念．合成法则记为加法的任意阿贝尔群 V 有唯一的方式构成 $\mathbb{Z}$ 上的一个模，由规则

$$nv = v + \cdots + v = \text{“}n\text{ 倍 }v\text{”}$$

及 $(-n)v = -(nv)$ 对任意正整数 n 定义．这些规则是由公理(1.1)赋予我们的，由 $1v=v$ 开始，它们的确把 V 做成一个 $\mathbb{Z}$-模；换言之，公理(1.1)成立．直观上这是非常容易接受的．要给出一个正式的证明，就得回到佩亚诺公理．反之，任意 $\mathbb{Z}$-模具有一个由忘却其标量积给出的阿贝尔群结构．这样

【1.2】 阿贝尔群和 $\mathbb{Z}$-模是等价的概念．

我们需要在阿贝尔群上用加法记号而使这个对应看起来是自然的．

整数环为我们提供了例子，以说明一个环上的模不必都是自由的．除了零群以外的有限阿贝尔群不同构于一个自由模 $\mathbb{Z}^n$，因为当 $n>0$ 时 $\mathbb{Z}^n$ 是无限的且 $\mathbb{Z}^0=0$．

本节剩下的部分将把一些基本术语拓广到模上．一个 R-模 V 的子模是一个在加法和标量乘法下封闭的非空子集．我们在前面已见到子模的一种情形，也就是理想．

【1.3】命题 R-模 R^1 的子模是 R 的理想.

证明 由定义，一个理想是 R 的一个在加法和与 R 中元素的乘积下封闭的子集. ■

R-模的同态的定义复制了向量空间的线性变换的定义. R-模的同态 $\varphi: V \longrightarrow W$ 是一个与合成法则相容的映射：

【1.4】 $$\varphi(v+v') = \varphi(v) + \varphi(v') \quad \text{和} \quad \varphi(rv) = r\varphi(v)$$

对所有 v, $v' \in V$ 及 $r \in R$ 成立. 一个双射的同态称为一个同构. 同态 $\varphi: V \longrightarrow W$ 的核是 V 的子模，φ 的象是 W 的子模.

对向量空间所给出的证明[第四章(2.1)]表明自由模的每个同态 $\varphi: R^m \longrightarrow R^n$ 是用元素属于 R 的矩阵左乘.

451

我们也需要将商群的概念拓广到模. 设 R 是环，并设 W 是一个 R-模 V 的一个子模. 商群 V/W 是陪集 $\overline{v} = v + W$ 的加法群[第二章(9.5)]. 用法则

【1.5】 $$r\overline{v} = \overline{rv}$$

将它做成一个 R-模. 我们在前面已经这样构造过几次. 现将需要用到的事实总结如下.

【1.6】命题

(a) 法则(1.5)是唯一定义的，且它使 $\overline{V} = V/W$ 成为一个 R-模.

(b) 使 $v \rightsquigarrow \overline{v}$ 的典范映射 π: $V \longrightarrow \overline{V}$ 是 R-模的一个满同态且其核为 W.

(c) 映射性质：设 f: $V \longrightarrow V'$ 是 R-模的一个其核包含 W 的同态. 存在唯一的同态 $\overline{f}$: $\overline{V} \longrightarrow V'$ 使得 $f = \overline{f}\pi$.

(d) 第一同构定理：如果 $\ker f = W$，则 $\overline{f}$ 是由 $\overline{V}$ 到 f 的象的一个同构.

(e) 对应定理：存在 $\overline{V}$ 的子模 $\overline{S}$ 与 V 的包含 W 的子模 S 间的一一对应，由 $S = \pi^{-1}(\overline{S})$ 和 $\overline{S} = \pi(S)$ 定义. 如果 S 与 $\overline{S}$ 是对应的模，则 V/S 与 $\overline{V}/\overline{S}$ 同构.

我们已知道关于群与正规子群类似的事实. 剩下需要验证的是标量乘法是唯一定义的，满足模的公理，以及与映射的相容. 这些验证可按前面所建立的方式进行.

第二节 矩阵、自由模和基

元素在一个环中的矩阵可以像元素在一个域中的矩阵那样进行运算. 即矩阵的加法和乘法像第一章中一样进行定义，而且它们满足相似的规则. 元素在环 R 中的矩阵通常称为一个 R-矩阵.

我们想知道哪些 R-矩阵是可逆的. 一个 $n \times n$ 的 R-矩阵的行列式可以用原来的任何一个规则加以计算. 利用完全展开式[第一章(4.12)]是方便的，因为它将行列式表成了 n^2 个矩阵元素的一个多项式. 于是记

452

【2.1】 $$\det A = \sum_p \pm a_{1p(1)} \cdots a_{np(n)},$$

这个和取遍集合$\{1, \cdots, n\}$的所有置换，符号 $\pm$ 代表置换的符号. 将这个公式在一个 R-矩阵上取值，得到 R 的一个元素. 通常的行列式规则仍成立，特别有

$$\det AB = (\det A)(\det B).$$

当矩阵元素属于一个域时我们已经证明这一规则[第一章(3.16)]，下一节将讨论这样的公式能搬到环的原因．我们假定它们可搬到环上．

如果 A 有元素属于 R 的乘法逆 A^{-1}，则有

$$(\det A)(\det A^{-1}) = \det I = 1.$$

这表明可逆 R-矩阵的行列式是环的单位．反之，设 A 是一个 R-矩阵，且其行列式是一个单位 δ. 则用克拉默法则可以找到其逆：$\delta I = A(\operatorname{adj} A)$，其中伴随矩阵可由 A 通过取其子式的行列式算出[第一章(5.4)]．这一规则在任意环上也成立．因而如果 δ 是单位，则可在 R 中将 A^{-1} 解出为

$$A^{-1} = \delta^{-1}(\operatorname{adj} A).$$

【2.2】推论 *元素属于 R 的 $n\times n$ 可逆矩阵是其行列式为单位的那些矩阵．它们构成一个群*

$$GL_n(R) = \{n\times n \text{ 可逆 } R\text{- 矩阵}\},$$

称之为 R 上的一般线性群．

当环 R 中单位不多时可逆矩阵的行列式必须是单位这一事实对于矩阵是一个很强的条件．例如，如果 R 是整数环，则行列式必为 ± 1．大多数整数矩阵是可逆的实矩阵，因而它们属于 $GL_n(\mathbb{R})$．但除非行列式为 ± 1，否则逆矩阵的元素不会是整数，因而其逆将不属于 $GL_n(\mathbb{Z})$．然而如果 $n>1$，则仍有相当多的可逆矩阵，这是因为初等矩阵

$$I + ae_{ij} = \begin{bmatrix} 1 & & a \\ & \ddots & \\ & & 1 \end{bmatrix}, \quad i\neq j, \quad a\in R,$$

行列式为 1．这些矩阵生成相当大的群．其他初等矩阵，即对换矩阵和矩阵

$$\begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & u & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix}, \quad u \text{ 是 } R \text{ 的单位}$$

也是可逆的．

我们现在回到环 R 上的模的讨论．基与无关性的概念(第三章第三节)可以不作改动地由向量空间搬到模上：称模 V 的一个有序元素集$(v_1, \cdots, v_k)$生成(或张成)V，如果每个 $v\in V$ 是一个线性组合

【2.3】
$$v = r_1 v_1 + \cdots + r_k v_k, \quad \text{其中 } r_i \in R.$$

在这种情形元素 v_i 称为*生成元*．如果模 V 有一个有限的生成元集，则称之为*有限生成的*．我们研究的大多数模都将是有限生成的．一个 $\mathbb{Z}$-模 V 为有限生成的当且仅当它是在第六章第八节意义下的有限生成阿贝尔群．

我们在第一节看到，模不必同构于模 R^k 中的任一个．然而，一个给定的模可以碰巧是这样的，这时也把它称为*自由模*．这样，一个有限生成模 V 是自由模，如果存在一个同构

$$\varphi: R^n \xrightarrow{\sim} V.$$

453

例如，$\mathbb{R}^2$ 中的格是自由$\mathbb{Z}$-模，而有限非零阿贝尔群不是自由的. 自由$\mathbb{Z}$-模也称为自由阿贝尔群. 自由模构成一个重要而自然的类，我们将首先研究它们. 从第五节开始研究一般模.

按照向量空间的定义，我们称模 V 的一个元素集合$(v_1, \cdots, v_n)$为无关的，如果非平凡的线性组合皆不为零，即如果下列条件成立：

【2.4】 如果 $r_1v_1+\cdots+r_nv_n=0$， 其中 $r_i\in R$，则对 $i=1,\cdots,n$ 有 $r_i=0$.

一个集合是一个基，如果它既是无关的又是一个生成元集. 标准基 $\boldsymbol{E}=(e_1, \cdots, e_k)$是 R^k 的一个基. 与向量空间完全一样的是，如果每个向量 $v\in R$ 可以用唯一一种方式写为线性组合(2.3)，则$(v_1, \cdots, v_k)$是一个基.

利用第三章第五节的术语，我们也可以讨论无限集合的线性组合及线性无关性.

如第三章第三节一样，用 $\boldsymbol{B}$ 表示有序集$(v_1, \cdots, v_n)$. 于是用 $\boldsymbol{B}$ 左乘

$$\boldsymbol{B}X=(v_1,\cdots,v_k)\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}=v_1x_1+\cdots+v_nx_n$$

定义一个模同态

【2.5】 $$\mu: R^n \longrightarrow V.$$

这个同态是满射当且仅当集合$(v_1, \cdots, v_n)$生成 V，而 μ 是单射当且仅当它是无关的. 因而它是双射当且仅当 $\boldsymbol{B}$ 是 V 的基，在这种情形下 V 是自由模. 因而一个模 V 有基当且仅当它是自由模. 大多数模都没有基.

454

自由 R-模用基的计算可以与向量空间用基计算以大致相同的方式进行，并利用元素属于 R 的矩阵. 特别是可以考虑一个元素 $v\in V$ 的关于基 $\boldsymbol{B}=(v_1, \cdots, v_n)$的坐标向量. 它是使得

$$v=\boldsymbol{B}X=v_1x_1+\cdots+v_nx_n$$

的唯一的列向量 $X\in R^n$.

如果给定同一个自由模 V 的两个基 $\boldsymbol{B}=(v_1, \cdots, v_n)$和 $\boldsymbol{B}'=(v_1', \cdots, v_r')$，则与第三章第四节同样地通过将第一个基的元素 v_j 写为第二个基的线性组合：$\boldsymbol{B}=\boldsymbol{B}'P$ 或

【2.6】 $$v_j=\sum_{i=1}^{r}v_i'p_{ij}$$

而得到基变换矩阵.

与向量空间一样，只要 R 不是零环，其自由模在非零环上的任意两个基都有相同的基数. 这样在上面的情形有 $n=r$. 这可以通过考虑由将 $\boldsymbol{B}'$表示为 $\boldsymbol{B}'=\boldsymbol{B}Q$ 而得到的逆矩阵 $Q=(q_{ij})$来证明. 于是

$$\boldsymbol{B}=\boldsymbol{B}'P=\boldsymbol{B}QP.$$

由于 $\boldsymbol{B}$ 是基，将 v_j 写成$(v_1, \cdots, v_n)$的线性组合的方式仅有一种，即 $v_j=1v_j$，或 $\boldsymbol{B}=\boldsymbol{B}I$. 因而 $QP=I$，类似地有 $PQ=I$：基变换矩阵是可逆的 R-矩阵.

如果 P 是 $r\times n$ 矩阵而 Q 是 $n\times r$ 矩阵. 假设 $r>n$. 则可通过加零而将 P 和 Q 做成方阵：

$$[P\mid 0]\left[\frac{Q}{0}\right]=I.$$

这并设有改变积 PQ. 但这些方阵的行列式为零，因为 $R\neq 0$，因而它们不可逆. 这表明 $r=n$，

正是我们所断言的.

令人惊讶的事实是存在非交换环 R，使得对 $n=1, 2, 3, \cdots$ 模 R^n 都是同构的(见杂题练习 6). 除非元素交换，否则行列式失效.

遗憾的是与向量空间相关的概念在用于环上的模时有另外的名字，现在要改变它们为时已晚. 自由模 V 的基元素的个数称为 V 的秩而不是维数.

正如我们已注意到的，列向量间的每个同态 $\varphi: R^n \longrightarrow R^m$ 是一个用矩阵 A 的左乘. 如果 $\varphi: V \longrightarrow W$ 是分别有基 $\mathbf{B}=(v_1, \cdots, v_n)$ 和 $\mathbf{C}=(w_1, \cdots, w_m)$ 的自由 R-模间的一个同态，则同态的矩阵定义为 $A=(a_{ij})$，其中像前面[第四章(2.3)]一样

【2.7】
$$\varphi(v_j) = \sum_i w_i a_{ij}.$$

455

用可逆 R-矩阵 P，Q 对基 **B**，**C** 作变换使 φ 的矩阵变为 $A' = QAP^{-1}$[第四章(2.7)].

第三节　恒等式的不变性原理

本节我们着重考虑下面的问题：为什么元素属于一个域的矩阵的性质对于元素属于一个任意环的矩阵仍然成立？简单地说，原因是它们是恒等式，也就是说当把矩阵元素换为变量时它们仍然成立. 更精确地说，假设想要证明如像行列式的乘法性质这样的恒等式，$(\det A)(\det B) = \det(AB)$，或克拉默法则等. 假如已对复元素矩阵验证了恒等式. 我们不想再重复一次，然而可能用到$\mathbb{C}$的特殊性质，如域的公理，即每个复多项式有一个根这一事实，或$\mathbb{C}$的特征为零等事实来验证恒等式. 我们的确用到过特殊性质来证明提到的恒等式，因而给出的证明对环不起作用. 我们现在指出如何从复数的恒等式对所有环推导出同样的恒等式.

原理是非常一般的，我们将专注于恒等式$(\det A)(\det B) = \det(AB)$的证明. 首先将矩阵元素用变量代替. 考虑同一个等式

$$(\det X)(\det Y) = \det(XY),$$

其中 X 和 Y 表示变量元素的 $n \times n$ 矩阵. 然后可以用任意环 R 的元素代入这些变量. 从形式上看，这个代入是以 $2n^2$ 个变量矩阵元素的整多项式环$\mathbb{Z}[\{x_{ij}\}, \{y_{ij}\}]$的语言来定义的. 存在唯一一个由整数环到任意环 R 的同态[第十章(3.9)]. 给定元素属于 R 的矩阵 $A=(a_{ij})$，$B=(b_{ij})$，存在一个同态

【3.1】
$$\mathbb{Z}[\{x_{ij}\}, \{y_{ij}\}] \longrightarrow R,$$

即替代同态，它使 $x_{ij} \rightsquigarrow a_{ij}$ 和 $y_{ij} \rightsquigarrow b_{ij}$[第十章(3.4)]. 我们的变量矩阵的元素属于多项式环，自然有同态使得 $X \rightsquigarrow A$ 和 $Y \rightsquigarrow B$，也就是说通过映射将 $X=(x_{ij})$的元素映到 $A=(a_{ij})$的元素，等等.

我们心目中的一般原理是：假如想要证明一个恒等式，其每一项都是矩阵元素的整系数多项式. 则其项与环同态相容：例如，如果一个同态 $\varphi: R \longrightarrow R'$使 $A \rightsquigarrow A'$ 及 $B \rightsquigarrow B'$，则它使 $\det A \rightsquigarrow \det A'$. 为此，注意行列式的完全展开式是

$$\det A = \sum_p \pm a_{1p(1)} \cdots a_{np(n)},$$

456

求和项在所有置换 p 上取. 由于 φ 是同态，

$$\varphi(\det A) = \sum_p \pm \varphi(a_{1p(1)} \cdots a_{np(n)}) = \sum_p \pm a_{1p(1)}{}' \cdots a_{np(n)}{}' = \det A'.$$

显然，这是个一般原理. 结果，如果恒等式对 R-矩阵 A，B 成立，则它也对 R'-矩阵 A'，B' 也成立.

现在对每一对矩阵 A，B，我们有同态(3.1)，它使得 $X \rightsquigarrow A$ 和 $Y \rightsquigarrow B$. 在刚才描述的原理中用$\mathbb{Z}[\{x_{ij}\},\{y_{ij}\}]$代替 R 而用 R 代替 R'. 我们得到如果恒等式对$\mathbb{Z}[\{x_{ij}\},\{y_{ij}\}]$中的变量矩阵 X，Y 成立，则它对任意环 R 的每一对矩阵成立：

【3.2】要一般地证明恒等式，只需对环$\mathbb{Z}[\{x_{ij}\},\{y_{ij}\}]$上的变量矩阵 X，Y 证明即可.

要对变量矩阵证明恒等式，我们将整数环视为复数域的子环，注意多项式环的包含关系

$$\mathbb{Z}[\{x_{ij}\},\{y_{ij}\}] \subset \mathbb{C}[\{x_{ij}\},\{y_{ij}\}].$$

455

也可在更大的环上验证恒等式. 现在根据假设，我们的恒等式等价于变量$\{x_{ij}\}$，$\{y_{ij}\}$，…的某些多项式的相等. 将恒等式写为 $f(x_{ij}, y_{ij})=0$. 符号 f 可以代表多个多项式.

现在考虑与多项式 $f(x_{ij}, y_{ij})$相对应的多项式函数，记为$\tilde{f}(x_{ij}, y_{ij})$. 如果对所有复矩阵证明了恒等式，则得到函数$\tilde{f}(x_{ij}, y_{ij})$是零函数. 应用一个多项式由它所定义的函数来确定这一事实[第十章(3.8)]可以得到 $f(x_{ij}, y_{ij})=0$，这就完成了证明.

在任意环上进行上面的讨论而证明关于恒等式成立的精确的定理是可能的. 然而，既使是数学家有时也感到不必作出精确的表述——当遇到每一具体情形再考虑有时会更容易些. 这里就是一个这样的情形.

第四节 整数矩阵的对角化

本节讨论用一序列初等变换化简一个 $m\times n$ 整数矩阵 $A=(a_{ij})$. 后面将应用这一过程来对阿贝尔群进行分类. 同样的方法也可应用到元素属于欧几里得整环的矩阵，通过适当的修改，也可用到元素属于主理想整环的矩阵.

457

如果同时进行行变换和列变换，我们可以得到最好的结果. 因而作这些变换：

【4.1】(i) 将一行的整数倍加到另一行，或将一列的整数倍加到另一列；

(ii) 交换两行或两列；

(iii) 用单位乘到一行或一列上.

当然，$\mathbb{Z}$ 的单位为± 1. 任何一个这样的变换可以通过将 A 左乘或右乘一个适当的初等整数矩阵实现. 一系列这样变换的结果具有

【4.2】
$$A' = QAP^{-1}$$

的形式，其中 $Q\in GL_m(\mathbb{Z})$和 $P^{-1}\in GL_n(\mathbb{Z})$是初等整数矩阵的乘积. 不用说，可以省去 P 上的取逆符号. 在这里使用逆是因为想把变换解释为基变换.

在一个域上，任意矩阵可由这样的变换变为块形式[第四章(2.9)]

$$A' = \begin{bmatrix} I & \\ & 0 \end{bmatrix}.$$

456

对于整数环我们不可能希望有这样一个结果. 即使1×1矩阵也不行. 但可以将其对角化.

【4.3】**定理** 设 A 是一个 $m\times n$ 整数矩阵. 存在如上的初等整数矩阵的积 P，Q 使得 $A'=QAP^{-1}$为对角矩阵

$$\begin{bmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{bmatrix} & \\ & 0 \end{bmatrix},$$

其中对角元素 d_i 是非负的且每个对角元素整除下一个：$d_1 \mid d_2$，$d_2 \mid d_3$，…．

证明 我们的策略是作一系列变换而最终得到矩阵

【4.4】
$$\begin{bmatrix} d_1 & 0 \cdots 0 \\ 0 & \\ \vdots & \begin{bmatrix} & & \\ & B & \\ & & \end{bmatrix} \\ 0 & \end{bmatrix},$$

其中 d_1 整除 B 的每一个元素．一旦做到这一点，就可以在 B 上继续．这一过程基于带余除法．我们将描述一个系统的方法，虽然这个方法通常不是最快的方法．

458

可以假设 $A \neq 0$．

第 1 步：通过置换行与列，将一个具有最小绝对值的非零项移到左上角．必要时在第一行乘上 -1 而使得这个左上角元素 a_{11} 为正．

现在消去第一行和第一列．当变换在矩阵中产生一个绝对值小于 $|a_{11}|$ 的非零元时，回到第 1 步并再次重复整个过程．这可能损坏已做的消去矩阵元素的工作．然而，因为每次都降低了 a_{11} 的大小，所以还是取得了进展．通常不会无限次地回到第 1 步．

第 2 步：在第一列选择一个使 $i>1$ 的非零元 a_{i1}，并用 a_{11} 整除：

$$a_{i1} = a_{11}q + r,$$

其中 $0 \leqslant r < a_{11}$．从(行 i)减去 q 倍(行 1)．这将 a_{i1} 变为 r．

如果 $r \neq 0$，回到第一步．如果 $r=0$，在第一列得到一个零．第 1 步和第 2 步的有限次重复给出一个对所有 $i>1$ 都有 $a_{i1}=0$ 的矩阵．同样地可以用类似于第 2 步的方法用列变换消去第一行，最终得到第一行和第一列只有 a_{11} 为非零元素的矩阵，这正是(4.3)所要求的．然而，a_{11} 可能还不能整除矩阵 B(4.4)的每个元素．

第 3 步：假设第一行和第一列只有 a_{11} 是非零元素，但 B 的某个元素 b 不被 a_{11} 整除．将 A 中包含 b 的列加到第一列．这样在第一列产生一个元素 b．

回到第 2 步．带余除法现在会产生一个更小的矩阵元素，从而回到第 1 步．这些步骤的有限序列将产生一个形如(4.4)的矩阵，使我们能用归纳法继续完成证明． ∎

【4.5】例 我们不按系统的方法来作：

$$A = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix} \xrightarrow[\text{变换}]{\text{列}} \begin{bmatrix} 1 & -1 \\ 3 & 2 \end{bmatrix} \xrightarrow[\text{变换}]{\text{列}} \begin{bmatrix} 1 & \\ 3 & 5 \end{bmatrix} \xrightarrow[\text{变换}]{\text{行}} \begin{bmatrix} 1 & \\ & 5 \end{bmatrix} = A'.$$

这里

$$Q = \begin{bmatrix} 1 & \\ -3 & 1 \end{bmatrix} \quad \text{而} \quad P^{-1} = \begin{bmatrix} 1 & \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}.$$

注意这个证明的关键是除法算法．当用任意欧几里得整环代替 $\mathbb{Z}$ 时证明仍是可行的．

【4.6】定理 设 R 是欧几里得整环，例如域上的一元多项式环 $F[t]$. 设 A 是一个元素属于 R 的 $m\times n$ 矩阵. 则存在初等 R-矩阵的积 P，Q，使得 $A'=QAP^{-1}$ 是对角矩阵并且使得 A' 的每个对角元素都整除下一个：$d_1|d_2|d_3|\cdots$. 如果 $R=F[t]$，我们可要求多项式 d_i 是首一的而使之正规化.

459

【4.7】例 多项式矩阵的对角化：

$$A=\begin{bmatrix}t^2-3t+2 & t-2\\ (t-1)^3 & t^2-3t+2\end{bmatrix}\xrightarrow[\text{变换}]{\text{行}}\begin{bmatrix}t^2-3t+2 & t-2\\ (t-1)^2 & 0\end{bmatrix}\xrightarrow[\text{变换}]{\text{行}}\begin{bmatrix}-t+1 & t-2\\ (t-1)^2 & 0\end{bmatrix}\xrightarrow[\text{变换}]{\text{列}}$$

$$\begin{bmatrix}-1 & t-2\\ (t-1)^2 & 0\end{bmatrix}\xrightarrow[\text{变换}]{\text{列}}\begin{bmatrix}-1 & 0\\ (t-1)^2 & (t-1)^2(t-2)\end{bmatrix}\xrightarrow[\text{变换}]{\text{行}}\begin{bmatrix}1 & \\ & (t-1)^2(t-2)\end{bmatrix}$$

$$=A'.$$

两个例子中，最后左上角为 1. 这并不令人吃惊. 矩阵元素的最大公因数常常为 1.

整数矩阵的对角化可用于描述自由阿贝尔群之间的同态. 如我们已经在(2.8)注意到的，一旦选定 V 和 W 的基，自由阿贝尔群的同态 $\varphi:V\longrightarrow W$ 由一个矩阵描述. V，W 由可逆整数矩阵 P，Q 给出的基变换将 A 变为 $A'=QAP^{-1}$. 这样，我们证明了下面的定理：

【4.8】定理 设 $\varphi:V\longrightarrow W$ 是自由阿贝尔群的同态. 存在 V 和 W 的基使得同态的矩阵具有对角形式(4.3).

在本节的剩余部分，我们将利用与一个同态相伴的两个辅助群：它的核及它的象来探讨这个定理的意义.

设 $\varphi:\mathbb{Z}^n\longrightarrow\mathbb{Z}^m$ 是用 $m\times n$ 整数矩阵 A 左乘. φ 的核是由线性方程组

【4.9】
$$AX=0$$

的整数解所构成的$\mathbb{Z}^n$ 的子群. 当矩阵为对角时解可以立即读出：要对 X 求解对角方程组 $d_1x_1=0$，$\cdots$，$d_nx_n=0$，我们必有 $x_i=0$，除非 $d_i\neq0$，而当 $d_i=0$ 时 x_i 可任意.

为了一般地解出方程(4.9)，我们可以对角化 A，比如对角化为 $A'=QAP^{-1}$，其中 Q，P 是初等整数矩阵的积. 作变量变换 $X'=PX$ 并且解对角方程组

$$A'X'=QAP^{-1}X'=0.$$

由于 Q 可逆，方程组 $QAX=0$ 与方程组 $AX=0$ 有相同的解. 因而原方程组的解为 $X=P^{-1}X'$.

其次我们考察如上用整数矩阵 A 左乘所定义的映射 $\varphi:\mathbb{Z}^n\longrightarrow\mathbb{Z}^m$ 的象. 可将这个象描述为使得整数方程组 $AX=B$ 有整数解的向量 $B\in\mathbb{Z}^m$ 的集合. 通常将这个象的集合记作 $A\mathbb{Z}^n$. 用 A 乘将基 e_1，$\cdots$，$e_n\in\mathbb{Z}^n$ 变到 A 的列

460

【4.10】
$$A_1=\begin{bmatrix}a_{11}\\ \vdots\\ a_{m1}\end{bmatrix},\quad\cdots,\quad A_n=\begin{bmatrix}a_{1n}\\ \vdots\\ a_{mn}\end{bmatrix},$$

因而象是这些列的整数线性组合的集合. 换言之，列生成象.

我们可将这个描述反过来，从一个由生成元 A_1，$\cdots$，$A_n\in\mathbb{Z}^m$ 具体给出的自由阿贝尔群$\mathbb{Z}^m$ 的任意子群 S 开始. 设 A 是其列为 A_i 的矩阵. 则 S 是用 A 左乘的象. S 的这个作为同态象的解释告诉我们用可逆整数矩阵 Q 和 P^{-1} 左乘和右乘的意义：用 Q 左乘对应于映射的值域，即

模$\mathbb{Z}^m$的基变换．其效果是每个生成元A_i乘上Q．另一方面，用P^{-1}右乘代表在定义域$\mathbb{Z}^n$中的基变换．这改变了S的生成元集．例如，将r乘上第一列加到第二列将A_2变为$A_2'=A_2+rA_1$而使其他生成元不变．将这些观察与对角化的结果结合起来得到下面的定理：

【4.11】定理　*设S是秩为m的自由阿贝尔群W的一个子群．存在W的基$(w_1, \cdots, w_m)$和S的基$(u_1, \cdots, u_n)$，具有下列性质：(i)$n \leqslant m$，(ii)对每个$j \leqslant n$，存在正整数d_j使得$u_j=d_j w_j$以及(iii)$d_1 \mid d_2 \mid d_3 \cdots$.*

【4.12】推论　*秩为m的自由阿贝尔群的每个子群都是自由的，并且其秩最多为m.*

定理(4.11)的证明　粗略地讲，我们只需为W选择一个基$\boldsymbol{B}=(w_1, \cdots, w_m)$，并为$S$选择一个生成元集$(u_1, \cdots, u_n)$，以得到一个如上的代表$S$的$m \times n$矩阵$A$．对角化定理给出一个代表$S$的关于新的基$\boldsymbol{B}'=(w_1', \cdots, w_m')$和新的生成元集$(u_1', \cdots, u_n')$的对角矩阵$A'=QAP^{-1}$．于是$u_j'=d_j'w_j'$．我们去掉最上面的那些而得到所需要的基和生成元集．除了下面三点，这就完成了证明．

第一点，可能会有$n>m$，即列数会比行数多．但如果这样的话，则由于A'是对角矩阵，对每一个$j>m$，其第j列皆为零，因此对应的生成元u_j也为零．零元作为生成元是没有用的，故可将其舍弃．同样的原因，只要$d_j=0$，就可舍弃一个生成元u_j．这样做了以后，所有d_j都为正且有$n \leqslant m$.

注意如果S是零子群，最后将舍弃所有的生成元．与向量空间一样，我们必须采用空集合生成零模这一约定，否则在定理的叙述中要特别提到这一种例外情形．

其次，我们验证如果选择基和生成元集使得$d_i>0$且$n \leqslant m$，则$(u_1, \cdots, u_n)$是S的一个基．由于它生成S，需要证明的是$(u_1, \cdots, u_n)$是无关的．我们将线性关系$r_1u_1+\cdots+r_nu_n=0$重写为$r_1d_1w_1+\cdots+r_nd_nw_n=0$的形式．由于$(w_1, \cdots, w_m)$是一个基，因此对每一$i$有$r_id_i=0$，而由于$d_i>0$，所以$r_i=0$.

最后一点更为严重：需要从S的一个生成元的有限集合开始．怎么知道存在这样的一个集合呢？有限生成的阿贝尔群的子群是有限生成的，这是一个事实．我们将在第五节证明这一点．目前定理只能是在加上S是有限生成的子群的假设之下得到．W是有限生成的这一假设是不能去掉的．

■

定理(4.11)是相当具体的．设S是由一个矩阵A的列生成的$\mathbb{Z}^m$的子群，并假设$A'=QAP^{-1}$是对角的．为了将S按定理所断言的形式表示出来，我们将这个等式写为

【4.13】
$$Q^{-1}A' = AP^{-1}$$

的形式并作如下解释：矩阵AP^{-1}的列构成S的新的生成元集．由于矩阵A'是对角的，(4.13)告诉我们新的生成元是Q^{-1}各列的倍数．将$\mathbb{Z}^m$的基由标准基变为由Q^{-1}各列构成的基．这个基变换的矩阵是Q[见第三章(4.21)]．则新的生成元是新的基元素的倍数．

例如，设S是例(4.5)中矩阵A的两列生成的$\mathbb{R}^2$的格：则

【4.14】
$$Q^{-1}A' = \begin{bmatrix} 1 & \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & \\ & 5 \end{bmatrix} = \begin{bmatrix} 1 & \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = AP^{-1}.$$

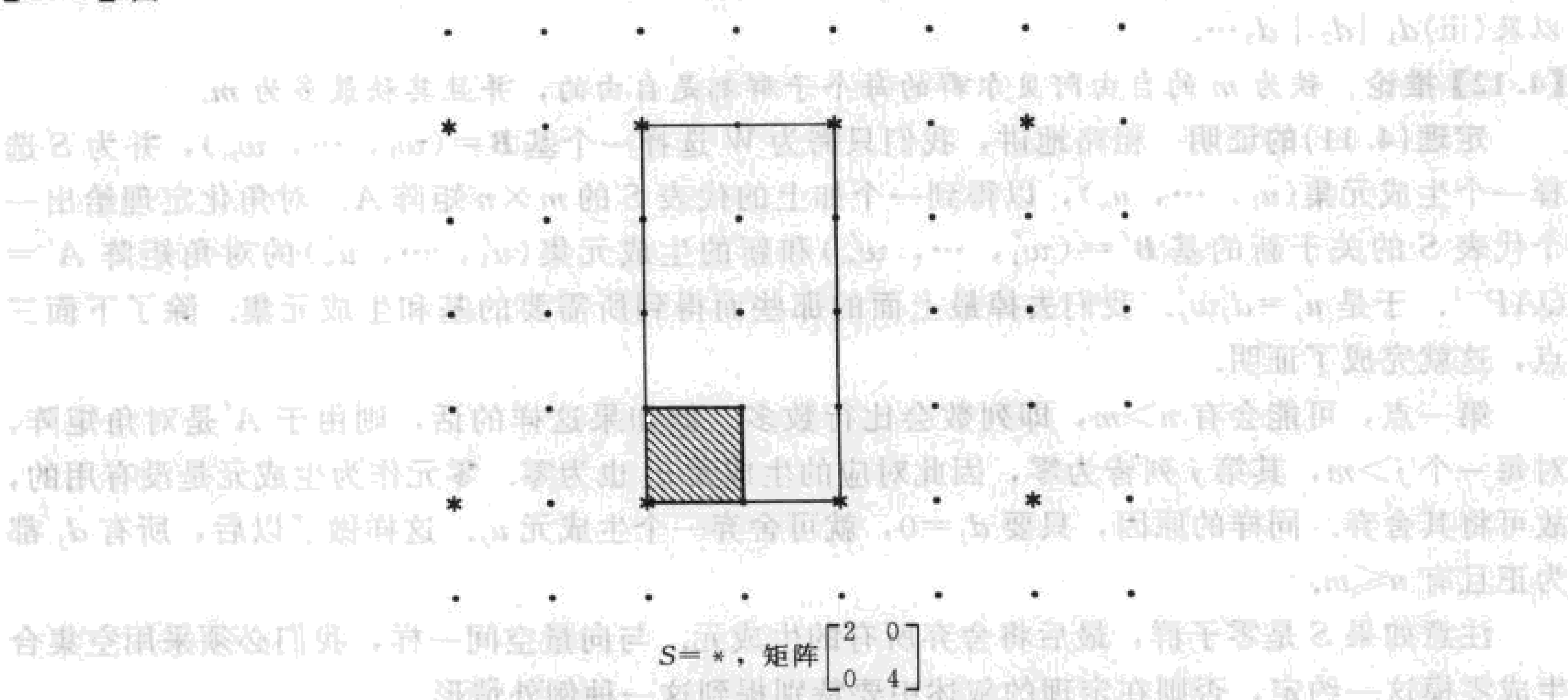
$\mathbb{Z}^2$的新基是$(w_1', w_2')=\left(\begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} \\ 1 \end{bmatrix}\right)$，而$S$的新生成元为$(u_1', u_2')=(u_1, u_2)P^{-1}=(w_1', 5w_2')$.

461

当用来描述子格 S 在格 L 中的相对位置时，定理(4.3)是令人惊讶的. 为阐明这点，我们只需考虑平面格. 定理断言存在 L 和 S 的基$(v_1,\ v_2)$和$(w_1,\ w_2)$使得 w_i 关于基$(v_1,\ v_2)$的坐标向量是对角的. 我们通过基$(v_1,\ v_2)$将格 L 归结到$\mathbb{Z}^2\subset\mathbb{R}^2$. 则等式 $w_i=d_iv_i$ 表明 S 看起来如下图所示，在其中取 $d_1=2$ 和 $d_2=4$：

462

【4.15】图

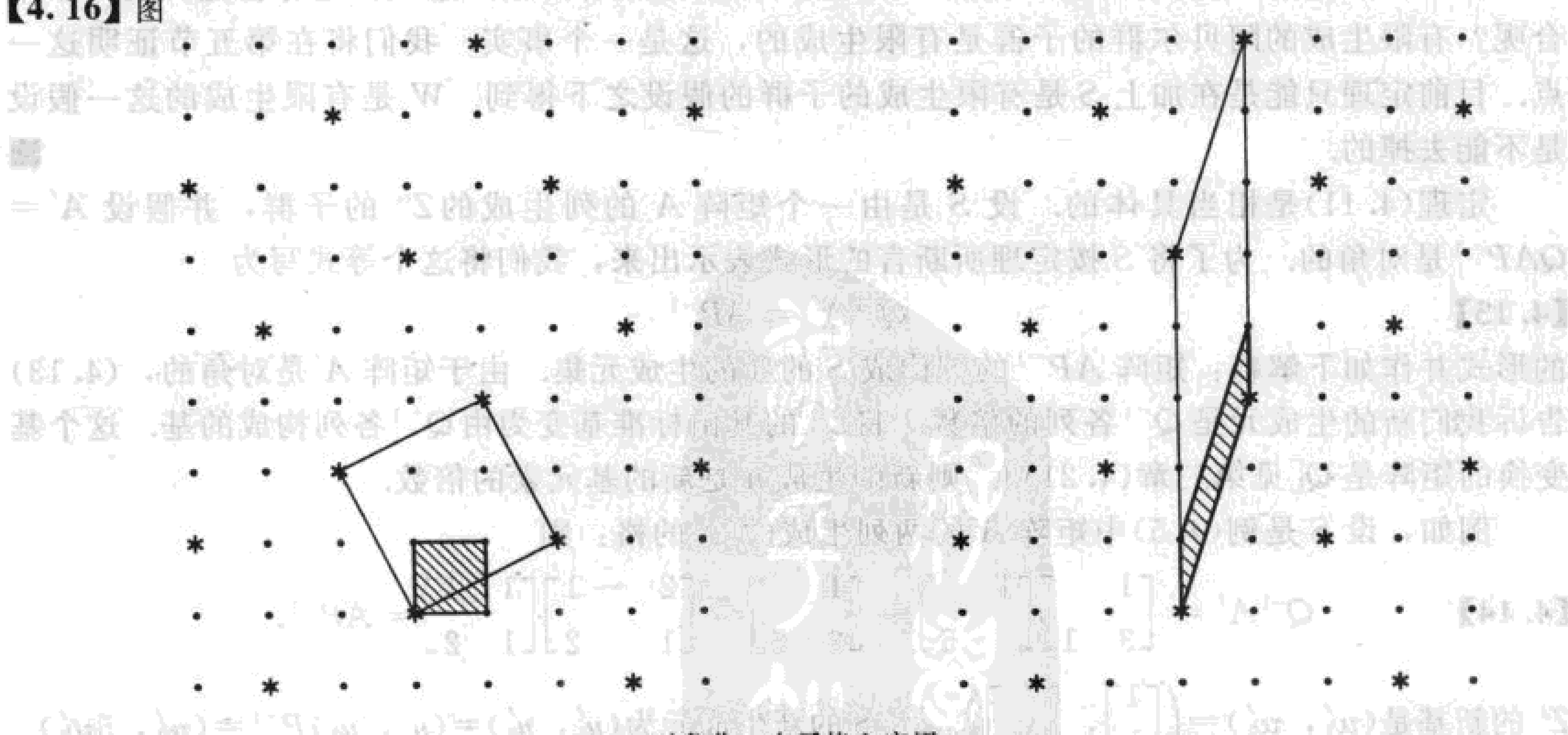


$S=*$，矩阵$\begin{bmatrix}2 & 0\\ 0 & 4\end{bmatrix}$

注意我们在前面所断言的事实[第十一章(10. 10)]，指标$[L:S]$是由基所张成的平行四边形的面积之比. 当基处于这样的相对位置时这一点是显然的.

实际上，当我们在开始时给定$\mathbb{R}^2$ 中的格 L 和 S 时，得到 L 和 S 的这样"互相度量"的基所需要的基变换导致相当长和相当细的平行四边形，对于例(4.14)如下面图形所示.

【4.16】图



463

第五节　模的生成元与关系

本节将注意力转到非自由的模．我们将指出如何用称之为*表现矩阵*的矩阵描述一大类模．然后把这些矩阵的对角化过程应用于阿贝尔群的研究．

作为要记住的一个例子，可以考虑由三个元素(v_1, v_2, v_3)生成的阿贝尔群或$\mathbb{Z}$-模V．假设这些生成元满足关系

【5.1】
$$\begin{aligned} 3v_1+2v_2+v_3&=0\\ 8v_1+4v_2+2v_3&=0\\ 7v_1+6v_2+2v_3&=0\\ 9v_1+6v_2+v_3&=0. \end{aligned}$$

描述这个模的关系归结为下列矩阵：

【5.2】
$$A=\begin{bmatrix}3&8&7&9\\2&4&6&6\\1&2&2&1\end{bmatrix},$$

其列是关系(5.1)的系数：

$$(v_1,v_2,v_3)A=(0,0,0,0).$$

和通常一样，标量出现在这个矩阵积的右边．这是我们计划中所要提出的描述模的方法．

如果$(v_1, \cdots, v_m)$为R-模V的元素，形如

【5.3】
$$a_1v_1+\cdots+a_mv_m=0,\quad a_i\in R$$

的等式称为元素间的*关系*．当然，在把(5.3)称作关系时，指的是形式表达式是关系：如果在V中取值，得到$0=0$．由于关系由R-向量$(a_1, \cdots, a_m)^t$确定，因此称这个向量为*关系向量*，指的是(5.3)在V中成立．一个关系的*完全集*是这样一个关系向量的集合：它使得每一关系向量都是这个集合的一个线性组合．显然，只有当形如(5.2)的矩阵的列向量构成一个关系的完全集时，这样一个矩阵才能完全地描述模V．

关系的完全集的概念会引起混乱．当使用自由模的同态而不是直接使用关系或关系向量时就会清楚得多．设给定一个元素属于环R的$m\times n$矩阵A．如我们熟知的，用这个矩阵的左乘是一个R-模同态

【5.4】
$$\varphi: R^n \longrightarrow R^m.$$

除了上节当$R=\mathbb{Z}$时所描述的同态的核和象以外，还有一个与R-模的同态$\varphi: W\longrightarrow W'$相伴的重要的辅助模，称为它的*余核*．$\varphi$的余核定义为商模

【5.5】
$$W'/(\operatorname{im}\varphi).$$

如果将用A左乘的象记为AR^n，则(5.4)的余核为R^m/AR^n．这个余核称为是由矩阵A*表现的*．更一般地，我们将任意同构

【5.6】
$$\sigma: R^m/AR^n \xrightarrow{\sim} V$$

称为模V的一个*表现*，如果存在一个这样的同构的话，矩阵A称为V的一个*表现矩阵*．

例如，循环群$\mathbb{Z}/(5)$是由1×1矩阵$[5]$表现的$\mathbb{Z}$-模. 作为另一个例子，设V是由矩阵$\begin{bmatrix}2&-1\\1&2\end{bmatrix}$表现的$\mathbb{Z}$-模. 这个矩阵的列是关系向量，因而$V$是由两个向量$v_1$，$v_2$生成，并且满足关系$2v_1+v_2=-v_1+2v_2=0$. 可以解出第一个关系得到$v_2=-2v_1$. 这使我们能消去第二个生成元. 代入第二个关系得到$-5v_1=0$. 因而V可由单独一个生成元v_1生成，满足单独一个关系$5v_1=0$. 这表明V同构于$\mathbb{Z}/(5)$. 这个2×2矩阵也表现循环群$\mathbb{Z}/(5)$.

现在将描述求给定模V的表现的一个理论方法. 要在实际中使用这个方法，需要有一种非常具体的方式给出模来. 第一步是选择生成元集$(v_1, \cdots, v_m)$. 因而从一开始V就必须是有限生成的. 这些生成元提供了一个将列向量$X=(x_1, \cdots, x_m)$映到$v_1x_1+\cdots+v_mx_m$的满同态

【5.7】
$$f:R^m\longrightarrow V.$$

f的核的元素是关系向量. 我们将这个核记为W. 由第一同构定理，模V同构于R^m/W.

重复这一过程，选择W的生成元集$(w_1, \cdots, w_n)$，并且像前面一样用这些生成元定义一个满同态

【5.8】
$$g:R^n\longrightarrow W.$$

因为W是R^m的子模，所以同态g与包含$W\subset R^m$的合成给出一个同态

【5.9】
$$\varphi:R^n\longrightarrow R^m.$$

这个同态就是用矩阵A左乘. 由构造，W是φ的象，也就是AR^n，所以$R^m/AR^n=R^m/W\approx V$. 因而A是V的表现矩阵.

465

矩阵A的列是我们取定的关系模W的生成元

$$w_1=\begin{bmatrix}a_{11}\\\vdots\\a_{m1}\end{bmatrix}, \quad \cdots, \quad w_n=\begin{bmatrix}a_{1n}\\\vdots\\a_{mn}\end{bmatrix}.$$

由于它们生成W，这些列构成模V的生成元$(v_1, \cdots, v_m)$的关系的完全集. 由于列是关系向量，因此

【5.10】
$$(v_1, \cdots, v_m)A=0.$$

这样模V的表现矩阵A由下列确定：

【5.11】

(i) V的一个生成元集，和

(ii) 这些生成元间的关系的完全集.

在这个描述中我们漏掉了一个要点. 要使关系模W有有限的生成元集合，这个模必须是有限生成的. 这看起来不像是一个令人满意的假设，因为原来的模V与W的关系是不清楚的. 我们不介意假设V是有限生成的，但要在一个在辅助构造中产生的模上加上假设条件是不好的. 我们需要更仔细地检查这一点[见(5.16)]. 但除了这点以外，可以对一个有限生成R-模V讨论它的生成元和关系.

由于表现矩阵依赖于选择(5.11)，因此许多矩阵表现同一个模，或者说同构的模. 下面是一些不会改变它所表现的模的同构类的变换矩阵A的规则：

【5.12】命题 设 A 是模 V 的一个 $m\times n$ 表现矩阵. 下列矩阵 A' 表现同一个模 V.

(i) $A'=QAP^{-1}$，其中 $Q\in GL_m(R)$ 而 $P\in GL_n(R)$；

(ii) A' 由删去一个零列得到；

(iii) A 的第 j 列是 e_i，而 A' 由 A 删去第 i 行和第 j 列得到.

证明

(i) 模 R^m/AR^n 同构于 V. 由于将 A 变到 QAP^{-1} 对应于改变 R^m 和 R^n 的基，因此商模的同构类没有改变.

(ii) 一个零列对应于平凡关系，故可以省去.

(iii) 假设矩阵 A 的第 j 列是 e_i. 对应的关系是 $v_i=0$. 因而这个等式在模 V 中成立，从而 v_i 可以从生成元集合$(v_1, \cdots, v_m)$中删去，对矩阵 A 作这样的改变就是删去第 i 行和第 j 列. 466 ■

通过这些规则可以将一个矩阵大大地简化. 例如，我们原来例子中的整数矩阵(5.2)可以如下化简：

$$A=\begin{bmatrix}3&8&7&9\\2&4&6&6\\1&2&2&1\end{bmatrix}\longrightarrow\begin{bmatrix}0&2&1&6\\0&0&2&4\\1&2&2&1\end{bmatrix}\longrightarrow\begin{bmatrix}2&1&6\\0&2&4\end{bmatrix}\longrightarrow\begin{bmatrix}2&1&6\\-4&0&-8\end{bmatrix}$$

$$\longrightarrow[-4\quad -8]\longrightarrow[-4\quad 0]\longrightarrow[4].$$

这样，A 表现阿贝尔群$\mathbb{Z}/(4)$.

由定义，一个 $m\times n$ 矩阵通过 m 个生成元和 n 个关系表现一个模. 但是正如在这个例子中所见到的，生成元的个数和关系的个数依赖于选择. 它们不是由模唯一确定的.

考虑另外两个例子：2×1 矩阵 $\begin{bmatrix}4\\0\end{bmatrix}$ 用两个生成元(v_1, v_2)和一个关系 $4v_1=0$ 表现一个阿贝尔群 V. 我们不能化简这个矩阵. 它表现的群与积群$\mathbb{Z}/(4)\times\mathbb{Z}$同构. 另一方面，矩阵$[4, 0]$表现一个有一个生成元和两个关系的群，第二个关系是平凡的. 这个群是$\mathbb{Z}/(4)$.

现在要讨论关系的模的有限生成的问题. 对于一个糟糕的环上的模，即使 V 是有限生成的，这个模也不一定是. 幸运的是对于我们所讨论的环这个问题不会发生，现在就证明这一点.

【5.13】命题 对一个 R-模 V，下列条件等价：

(i) V 的每个子模 W 都是有限生成的；

(ii) 升链条件：不存在 V 的子模的无限严格升链 $W_1<W_2<\cdots$.

证明 假设 V 满足升链条件，并设 W 是 V 的子模. 我们以下面的方式选择 W 的一个生成元集 $w_1, w_2, \cdots, w_k$：如果 $W=0$，则 W 由空集合生成. 否则就从一个非零元 $w_1\in W$ 开始. 继续下去，假设已选取 $w_1, \cdots, w_i$，并设 W_i 是由这些元素生成的子模. 如果 W_i 是 W 的一个真子模，设 w_{i+1} 是 W 中一个不含于 W_i 的元素. 则有 $W_1<W_2<\cdots$. 由于 V 满足升链条件，这个子模链不会无限制地继续下去. 因而某个 W_k 必等于 W. 这时$(w_1, \cdots, w_k)$生成 W. 其逆由第十一章定理(2.10)的证明得到. 假设 V 的每个子模都是有限生成的，并设 467

$W_1 \subset W_2 \subset \cdots$ 是 V 的子模的一个无限升链. 用 U 表示这些子模的并. 则 U 是一个子模[见第十一章(2.11)]; 因此它是有限生成的. 设 u_1, …, u_r 为 U 的生成元, 每个 u_ν 属于子模 W_i 中的一个, 而由于链是上升的, 存在一个 i 使得所有生成元都属于 W_i. 于是它们生成的模 U 也属于 W_i, 并且我们有 $U \subset W_i \subset W_{i+1} \subset U$. 这表明 $U = W_i = W_{i+1}$, 因而链不是严格上升的. ■

【5.14】引理

(a) 设 $\varphi: V \longrightarrow W$ 是 R-模同态. 如果 φ 的核与象是有限生成的模, 则 V 也是有限生成的模. 如果 V 是有限生成的且 φ 是满射, 则 W 是有限生成的. 更准确地说, 假设$(v_1, \cdots, v_n)$生成 V 且 φ 是满射, 则$(\varphi(v_1), \cdots, \varphi(v_n))$生成 W.

(b) 设 W 是 R-模 V 的子模. 如果 W 和 V/W 都是有限生成的, 则 V 也是有限生成的. 如果 V 是有限生成的, 则 V/W 也是有限生成的.

证明 对(a)的第一个断言, 我们遵循线性变换的维数公式的证明[第四章(1.5)], 选择 $\ker\varphi$ 的一个生成元集$(u_1, \cdots, u_k)$和 $\mathrm{im}\varphi$ 的一个生成元集$(w_1, \cdots, w_m)$. 我们还选择元素 $v_i \in V$ 使得 $\varphi(v_i) = w_i$. 则称集合$(u_1, \cdots, u_k; v_1, \cdots, v_m)$生成 V. 设 $v \in V$ 为任意元. 则 $\varphi(v)$是$(w_1, \cdots, w_m)$的线性组合, 设 $\varphi(v) = a_1 w_1 + \cdots + a_m w_n$. 令 $v' = a_1 v_1 + \cdots + a_m v_m$. 则 $\varphi(v) = \varphi(v')$. 于是 $v - v' \in \ker\varphi$, 因而 $v - v'$ 是$(u_1, \cdots, u_k)$的线性组合, 设 $v - v' = b_1 u_1 + \cdots + b_k u_k$. 于是 $v = a_1 v_1 + \cdots + a_m v_m + b_1 u_1 + \cdots + b_k u_k$. 这表明集合$(u_1, \cdots, u_k; v_1, \cdots, v_m)$生成 V, 这正是我们要证的. (a)的第二个断言容易证明. (b)通过考虑典范同态 π: $V \longrightarrow V/W$ 而由(a)得到. ■

【5.15】定义 环 R 称为诺特的, 如果它的每个理想都是有限生成的.

主理想整环显然是诺特环, 因而环$\mathbb{Z}$, $\mathbb{Z}[i]$及 $F[x]$(F 是域)是诺特环.

【5.16】推论 设 R 是诺特环. R 的每个真理想 I 包含在一个极大理想中.

证明 如果 I 自己不是极大理想, 则它真包含在一个真理想 I_2 中且如果 I_2 不是极大理想, 则它真包含在一个真理想 I_3 中, 等等. 由升链条件(5.13), 链 $I = I_1 < I_2 < I_3 < \cdots$ 必有限. 因而有某个 k 使得 I_k 是极大理想. ■

468

下列命题显示了诺特环的概念与我们的问题的关联:

【5.17】命题 设 V 是诺特环 R 上的一个有限生成模. 则 V 的每个子模都是有限生成的.

证明 只需对 $V = R^m$ 的情形证明命题. 因为假如对所有 m 证明了 R^m 的子模都是有限生成的. 设 V 是有限生成 R-模. 则存在满射 $\varphi: R^m \longrightarrow V$. 给定 V 的子模 S, 设 $L = \varphi^{-1}(S)$. 则 L 是 R^m 的子模, 因此 L 是有限生成的. 并且映射 $L \longrightarrow S$ 是满射. 因此 S 是有限生成的(5.14).

当 $V = R^m$ 时要证明命题, 我们对 m 作归纳. R 的一个子模和 R 的理想是同一回事(1.3). 这样 R 是诺特环的假设告诉我们当 $m = 1$ 时, 命题对 $V = R^m$ 成立. 假设 $m > 1$. 考虑由去掉最后一个元素给出的投射

$$\pi: R^m \longrightarrow R^{m-1}$$

$\pi(a_1, \cdots, a_m) = (a_1, \cdots, a_{m-1})$. 其核为$\{(0, \cdots, 0, a_m)\} \approx R$. 设 $W \subset R^m$ 是一个子模, 并设 $\varphi: W \longrightarrow R^{m-1}$ 是 π 在 W 上的限制. 由归纳假设, 象 $\varphi(W)$是有限生成的. 而 $\ker\varphi = (W \cap$

$\ker\pi$)是 $\ker\pi\approx R$ 的子模，因而它亦是有限生成的. 由引理(5.14)，W 是有限生成的，这正是要证的. ■

这个命题完成了定理(4.11)的证明.

由于主理想整环是诺特环，在这些环上有限生成模的子模是有限生成的. 但事实上，我们所讨论的大多数环都是诺特环. 这由希尔伯特的另一个著名定理得到：

【5.18】定理 希尔伯特基定理：如果环 R 是诺特环，则多项式环 $R[x]$ 也是.

由归纳法，希尔伯特基定理指出诺特环 R 上的多个变量的多项式环 $R[x_1, \cdots, x_n]$ 是诺特环，因此环 $\mathbb{Z}[x_1, \cdots, x_n]$ 和 $F[x_1, \cdots, x_n]$(F 为域)是诺特环. 而且，诺特环的商环都是诺特环：

【5.19】命题 设 R 是诺特环，并设 I 是 R 的理想. 商环 $\overline{R}=R/I$ 是诺特环.

证明 设 $\overline{J}$ 是 $\overline{R}$ 的理想，并设 $J=\pi^{-1}(\overline{J})$ 是对应的 R 的理想，其中 π：$R\longrightarrow\overline{R}$ 是典范映射. 则 J 是有限生成的，如由 $(a_1, \cdots, a_m)$ 生成. 由此得到有限集合 $(\overline{a}_1, \cdots, \overline{a}_m)$ 生成 $\overline{J}$(5.14). ■

469

将此命题与希尔伯特基定理结合起来得到下面的结果：

【5.20】推论 整数多项式环或域上的多项式环上的任意商环是诺特环.

希尔伯特基定理的证明 假设 R 是诺特环，并设 I 是多项式环 $R[x]$ 的理想. 必须证明有限个多项式的集合足以生成这个理想.

我们复习一下 R 为域的情形. 在这一情形，可以选择一个次数最低的非零多项式 $f\in I$，比如

【5.21】
$$f(x)=a_nx^n+\cdots+a_1x+a_0,\quad a_n\neq 0,$$

并如下证明它生成理想：设

【5.22】
$$g(x)=b_mx^m+\cdots+b_1x+b_0,\quad b_m\neq 0$$

为 I 的非零元素. 则 g 的次数 m 最小为 n. 对 m 作归纳. 多项式

【5.23】
$$g(x)-(b_m/a_n)x^{m-n}f(x)=g_1(x)$$

是 I 的次数 $<m$ 的元素. 由归纳假设，g_1 为 f 整除；因此 g 被 f 整除.

公式(5.23)是 g 由 f 作带余除法的第一步. 由于带余除法要求 f 的首项系数是单位，因此这个方法并不能直接拓广到任意环上. 更准确地说，为了构造表达式(5.23)，需要知道在环 R 中 a_n 能够整除 b_m，但没有理由保证这是对的. 我们将需要更多的生成元.

用 A 表示 I 中所有多项式的首项系数的集合并加上 R 的零元素.

【5.24】引理 $R[x]$ 的一个理想中多项式的首项系数的集合 A 与零一起构成 R 的一个理想.

证明 如果 $\alpha=a_n$ 是 f 的首项系数，则除非碰巧 $r\alpha=0$，否则 $r\alpha$ 就是 rf 的首项系数. 在这两种情形，都有 $r\alpha\in A$. 然后，设 $\alpha=a_n$ 是 f 的首项系数并设 $\beta=b_m$ 是 g 的首项系数，其中设 $m\geqslant n$. 则 α 亦是 $x^{m-n}f$ 的首项系数. 因此 x^m 在多项式 $h=x^{m-n}f+g$ 中的系数是 $\alpha+\beta$. 它或者是零，或者是 h 的首项系数，在这两种情形都有 $\alpha+\beta\in A$. ■

我们回到希尔伯特基定理的证明. 根据引理，集合 A 是诺特环 R 的理想，因而这个理想有一个有限生成元集，设为 $(\alpha_1, \cdots, \alpha_k)$. 对每个 i，$1\leqslant i\leqslant k$，选取一个首项系数为 α_i 的多项式 $f_i\in I$，必要时在这些多项式上乘上 x 的一个幂，使它们的次数都等于某个公共的整数 n.

470

这样得到的多项式集合$(f_1, \cdots, f_k)$能够用来改进归纳步骤(5.23)，但它可能不会生成I. 在理想$(f_1, \cdots, f_k)$中找到次数$<n$的多项式的机会不大. 因而必须加上一些低次元以得到理想的生成元. 下面的引理是容易的，我们略去其证明.

【5.25】引理　设P_n是$R[x]$中次数$<n$的多项式加上零的集合，并设$S_n = I \cap P_n$. 则S_n是R-模P_n的R-子模.

R-模P_n由单项式$1, x, \cdots, x^{n-1}$生成，因而它是有限生成的. 由于R是诺特的，可用引理(5.25)和命题(5.17)得出存在有限元素集合$(h_1, \cdots, h_s)$，它生成S_n作为R-模. 我们断言合起来的集合$(f_1, \cdots, f_k; h_1, \cdots, h_s)$生成$I$.

用J表示由这个集合生成的理想. 由构造，$J \subset I$. 我们需要证明相反的包含关系，对一个元素$g \in I$的次数进行归纳. 将这个次数记作m. 如果$m < n$，则$g \in S_n$，因而g是$(h_1, \cdots, h_s)$的系数属于R的线性组合. 因而在这种情形下$g \in J$. 假设$m \geqslant n$，设g的首项系数为$b = b_m$. 则b属于首项系数的理想A，因而它是该理想生成元的线性组合，设为$b = r_1\alpha_1 + \cdots + r_k\alpha_k$. 记住$\alpha_i$是$f_i$的首项系数，我们看到多项式

$$p = x^{m-n}\left(\sum_i r_i f_i\right)$$

与g有相同的首项系数和相同的次数，并且属于J. 于是$g_1 = g - p$的次数小于m. 由归纳假设，$g_1 \in J$，因此$g \in J$. ■

第六节　阿贝尔群的结构定理

阿贝尔群的结构定理断言有限生成阿贝尔群V是循环群的直和. 证明工作已经完成. 我们知道存在一个对角矩阵来表现V，剩下要做的是对于群解释这个对角矩阵的意义.

首先需要把直和的概念从向量空间拓广到任意的模. 定义是相同的. 设$W_1, \cdots, W_k$是模V的子模. 它们的和是由它们生成的子模. 它由所有的和

【6.1】
$$W_1 + \cdots + W_k = \{v \in V \mid v = w_1 + \cdots + w_k, \text{其中 } w_i \in W_i\}$$

组成. 验证这是子模是常规的，并且与向量空间的和的验证方法是一样的. 我们说V是子模471W_i的直和，如果

【6.2】

(i) 它们生成：$V = W_1 + \cdots + W_k$；

(ii) 它们是无关的：如果$w_1 + \cdots + w_k = 0$且$w_i \in W_i$，则对每个i有$w_i = 0$.

这样V是子模W_i的直和，如果每个元素$v \in V$可以唯一写成$v = w_1 + \cdots + w_k$的形式，其中$w_i \in W_i$. 与向量空间一样，两个子模W_1, W_2是无关的当且仅当$W_1 \cap W_2 = 0$[见第三章(6.5)].

和前面一样，用符号$\oplus$表示直和. 因而记号

【6.3】
$$V = W_1 \oplus \cdots \oplus W_k$$

表明V是子模W_i的直和.

【6.4】定理　阿贝尔群结构定理：设V是有限生成阿贝尔群. 则V是有限循环子群$C_{d_1}, \cdots,$

C_{d_k}和一个自由阿贝尔群L的直和：

$$V = C_{d_1} \oplus \cdots \oplus C_{d_k} \oplus L,$$

其中C_{d_i}的阶d_i大于1，且$d_1 \mid d_2 \mid d_3 \cdots$.

这里用加法记号表示循环群的合成法则．因而C_n由一个元素v生成，有一个关系$nv=0$．这样C_n同构于$\mathbb{Z}/(n)$．同构$\mathbb{Z}/(n) \longrightarrow C_n$将整数$r$的剩余映到$rv$.

定理的证明　选择V的由一个生成元集合和一个关系的完全集确定的表现矩阵A．我们可以这样做是因为V是有限生成的并且$\mathbb{Z}$是诺特环(见第五节)．由命题(5.12)，矩阵A可以由QAP^{-1}代替，其中Q和P是可逆的．因而可以假设A是对角的，其对角元是非零的，并且每个对角元整除下一个．而且可以去掉任意一个零列和任意其对角元为1的行和列(5.12)．因而，可以假定对角元d_i不是1或0．矩阵A具有形状

【6.5】

$$\begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_k \\ \hline & & 0 & \end{bmatrix}$$

因而它是一个$m \times k$矩阵，其中$k \leqslant m$．这对我们的模用生成元和关系的语言来说就是V由m个元素$v_1, \cdots, v_m$生成，而且 472

【6.6】

$$d_1 v_1 = 0, \quad d_2 v_2 = 0, \quad \cdots, \quad d_k v_k = 0$$

构成这些生成元之间关系的完全集合.

对于$j=1, \cdots, k$，我们用C_j表示由v_j生成的循环子群．设L是由剩下的生成元$v_{k+1}, \cdots, v_m$生成的子群．由于(6.5)的列是关系的完全集合，因此没有涉及后$m-k$个生成元的关系．因而L是秩为$m-k$的自由阿贝尔群．现在验证$V=C_{d_1} \oplus \cdots \oplus C_{d_k} \oplus L$和$C_j$是$d_j$阶循环群．首先，由于$V$由$v_i$生成且由于$v_i$中的每一个包含在直和项中的一个中，显然$V$是这些子群的和．其次，假定有一个关系，比如

$$z_1 + \cdots + z_k + w = 0,$$

其中$z_j \in C_j$且$w \in L$．由于C_j是由v_j生成的循环群，因而可以找到整数r_j使得$z_j = r_j v_j$．类似地，也可以找到整数r_j使得$w = r_{k+1} v_{k+1} + \cdots + r_m v_m$．则关系具有形式

$$r_1 v_1 + \cdots + r_m v_m = 0.$$

由于(6.5)的列构成关系的完全集，向量$(r_1, \cdots, r_m)^t$是这些列的线性组合．因而如果$j>k$有$r_j=0$，则这蕴涵$w=0$．另外，如果$j \leqslant k$，则r_j必为d_j整除，设$r_j = d_j s_j$．于是$z_j = s_j d_j v_j = 0$．这样关系是平凡的，并且表明子群是无关的．这也说明循环群C_j的阶是d_j．因而我们有$V=C_{d_1} \oplus \cdots \oplus C_{d_k} \oplus L$，这正是所要求的. ■

一个有限阿贝尔群是有限生成的，因而如上面所述，结构定理将有限阿贝尔群分解为有限循环群的直和，其中每个直和项的阶整除下一个的阶．这时自由阿贝尔群的直和项为零．有时将循环群进一步分解为素数幂阶循环群的直和更为方便．这一分解基于第二章的命题(8.4)，我们将其复述如下：

【6.7】 设r, s为互素整数．rs阶循环群C_n是r阶和s阶循环群的直和.

把这个引理和结构定理合起来，就得到下面的结果：

【6.8】推论 结构定理的另一形式：每一有限生成阿贝尔群是素数幂阶循环群与一个自由阿贝尔群的直和.

473 自然要问，在分解中将一个给定的有限阿贝尔群分解的循环子群的阶是否由群唯一确定. 如果 V 的阶是不同的素数的积，这没有问题. 例如如果阶为 30，则 V 必同构于 $C_2 \oplus C_3 \oplus C_5$. 但同一个群是否可能既是 $C_2 \oplus C_2 \oplus C_4$ 又是 $C_4 \oplus C_4$ 呢？通过比较 1 阶和 2 阶元素的个数不难证明这是不可能的. 群 $C_4 \oplus C_4$ 含有四个这样的元素而 $C_2 \oplus C_2 \oplus C_4$ 含有八个. 这种比较元素个数的方法总是很有效的.

【6.9】定理 结构定理的唯一性：

(a) 假设一个有限阿贝尔群 V 是循环群的直和：$C_{d_1} \oplus \cdots \oplus C_{d_k}$，其中 $d_1 \mid d_2 \mid d_3 \cdots$. 整数 d_j 由群 V 确定.

(b) 分解为素数幂阶(循环群直和)时，即每个 d_j 是一个素数的幂时同样的结论亦成立.

我们将证明留作练习.

通过将直和表为一个直积可使元素的计数得到记号上的简化. 设 R 是环. R-模 W_1，…，W_k 的直积是 k-重积集 $W_1 \times \cdots \times W_k$：

【6.10】
$$W_1 \times \cdots \times W_k = \{(w_1, \cdots, w_k) \mid w_i \in W_i\}.$$

它在向量加法和标量乘法之下构成一个模：

$$(w_1, \cdots, w_k) + (w'_1, \cdots, w'_k) = (w_1 + w'_1, \cdots, w_k + w'_k), \quad r(w_1, \cdots, w_k) = (rw_1, \cdots, rw_k).$$

模公理的验证是常规的.

下面定理指出直积和直和是同构的：

【6.11】命题 设 W_1，…，W_k 是 R-模 V 的子模.

(a) 由

$$\sigma(w_1, \cdots, w_k) = w_1 + \cdots + w_k$$

定义的映射 σ: $W_1 \times \cdots \times W_k \longrightarrow V$ 是一个 R-模同态，其象是和 $W_1 + \cdots + W_k$.

(b) 同态 σ 是同构当且仅当 V 是子模 W_i 的直和.

前面我们已多次看到类似的论证，因而省去其证明. 注意到命题的第二部分类似于下面的论述：由集合$(v_1$，…，$v_k)$定义的映射(2.5)$R^k \longrightarrow V$ 是一一映射当且仅当这个集合是一个基.

474 由于 d 阶循环群 C_d 同构于标准循环群$\mathbb{Z}/(d)$，因此可用命题(6.11)将结构定理复述如下：

【6.12】定理 结构定理的积形式：每个有限生成阿贝尔群 V 同构于循环群的直积

$$\mathbb{Z}/(d_1) \times \cdots \times \mathbb{Z}/(d_k) \times \mathbb{Z}^r,$$

其中 d_i，r 是整数. 存在一个其中每个 d_i 整除下一个的分解和一个其中每个 d_i 是素数幂的分解.

阿贝尔群的这个分类可以搬到欧几里得整环而没有本质改变. 由于欧几里得整环 R 是诺特环，任意有限生成 R-模 V 有一个表现矩阵(5.6)，由对角化定理(4.6)，存在一个对角的表现矩阵.

要保持与阿贝尔群的类似，我们定义循环 R-模 V 为由单独一个元素生成的子模. 这等价于说 V 同构于商模 R/I，其中 I 是 R 中使 $\alpha v = 0$ 的元素 α 的理想. 就是说由于 v 生成 V，使

$r \rightsquigarrow rv$的映射$\varphi: R \longrightarrow V$是模的满同态，且$\varphi$的核，即关系模是$R$的子模，也就是一个理想(1.3)．因而由第一同构定理，V同构于R/I．反之，如果$R/I \longrightarrow V$是一个同构，则1的象生成V．如果R是欧几里得整环，则理想I是一个主理想，因而对某个$\alpha \in R$，V将同构于$R/(\alpha)$．在这种情形下关系模将由单独一个元素生成．

下列定理可以和阿贝尔群的情形一样地加以证明：

【6.13】定理 欧几里得整环上模的结构定理：

(a) 设V是欧几里得整环R上的有限生成模．则V是循环模C_j和一个自由模L的直和．等价地，存在一个V与循环模$R/(d_i)$和自由模R^r的直积的同构

$$\varphi: V \longrightarrow R/(d_1) \times \cdots \times R/(d_k) \times R^r,$$

其中r非负，元素$d_1, \cdots, d_k$不是单位也不等于零，且对$i=1, \cdots, k-1$有d_i整除d_{i+1}．

(b) 与(a)同样的断言，只是将d_i整除d_{i+1}的条件改为每个d_i是R的素元素的幂．这样V同构于一个形如

$$R/(p_1^{e_1}) \times \cdots \times R/(p_n^{e_n}) \times R^r$$

的积，其中素元素的重复是允许的．

例如，考虑由例(4.7)的矩阵A表现的$F[t]$-模V．根据(5.12)，它也由对角矩阵

$$A' = \begin{bmatrix} 1 & \\ & (t-1)^2(t-2) \end{bmatrix}$$

475

表现，并且可以从这个矩阵(5.12)去掉第一行和第一列．因而V由1×1矩阵$[g]$表现，其中$g(t)=(t-1)^2(t-2)$．这表明V是循环模且同构于$F[t]/(g)$．由于g有两个互素的因子，因而V可以进一步分解．它同构于两个循环模的直积

【6.14】 $$V \approx F[t]/(g) \approx [F[t]/(t-1)^2] \times [F[t]/(t-2)].$$

通过稍微再进一步的工作，可以把定理(6.13)拓广到任意主理想整环的模．(b)中出现的素数幂除去单位因子是唯一的这一性质在这一情形也成立．必须找到一个代替证明定理(6.9)的计数的方法来证明这个事实．我们将不加以证明．

第七节 对线性算子的应用

本节我们以一种新奇的方式将上节发展的理论应用到域上向量空间的线性算子上．这一应用为“证明分析”产生数学中的新结果的方法提供了一个很好的例子．最初是对阿贝尔群提出的方法形式地推广到了欧几里得整环上模的情形．然后将它应用到多项式环的具体情形．这并不是历史的发展过程．阿贝尔群和线性算子的理论是独立发展的，后来才联系起来．但令人惊讶的是两种情形(阿贝尔群和线性算子)可以在形式上相似而当同样的理论在它们之上应用时最终产生看起来是如此不同的结果．

我们能够着手进行讨论的一个关键事实是如果给定域F上向量空间的一个线性算子

【7.1】 $$T: V \longrightarrow V,$$

则可以用这个算子将V构造成多项式环$F[t]$上的一个模．为此，需要定义一个多项式$f(t)=a_nt^n+\cdots+a_1t+a_0$与向量$v$的乘法．令

【7.2】 $$f(t)v=a_nT^n(v)+a_{n-1}T^{n-1}(v)+\cdots+a_1T(v)+a_0v.$$
右边可以记为$[f(T)](v)$，其中$f(T)$表示由将T代入t得到的线性算子$a_nT^n+a_{n-1}T^{n-1}+\cdots+a_1T+a_0I$. 加上括号只是为了清楚. 用这个记号得到公式

【7.3】 $$tv=T(v) \quad \text{和} \quad f(t)v=[f(T)](v).$$
规则(7.2)使V成为一个$F[t]$-模这个事实是容易验证的. 公式(7.3)看起来没有什么特别的地方. 它们导致了为什么需要一个新符号t的问题. 但要记住$f(t)$是形式多项式而$f(T)$表示的是某个线性算子.

反之，设V是一个$F[t]$-模. 则V的元素由多项式$f(t)$来作标量乘法是有定义的. 特别是我们得到一个常数多项式，即F中元素的乘法的法则. 如果保持常数乘法法则而暂时忘掉非常数多项式的乘法，则公理(1.1)表明V成为F上的一个向量空间. 其次，可以用多项式t乘V的元素. 将t在V上的乘法作用表示为T. 则T是映射

476

【7.4】 $$T:V\longrightarrow V, \quad \text{定义为} \quad T(v)=tv.$$
当将V视为F上的向量空间时，这个映射是它上面的一个线性算子. 因为由分配律(1.1)，$t(v+v')=tv+tv'$，因此$T(v+v')=T(v)+T(v')$. 而且如果$c\in F$，则由结合律(1.1)和$F[t]$中的交换律，有$tcv=ctv$；因此$T(cv)=cT(v)$. 因而一个$F[t]$-模给出向量空间上的一个线性算子.

我们描述的这些作用，从线性算子到模及其反过来，是互逆的：

【7.5】 *F-向量空间上的线性算子与$F[t]$-模是等价概念.*

我们将把这个事实应用于有限维向量空间，但顺便注意一下对应于秩为1的自由$F[t]$-模$F[t]$的线性算子. 我们知道$F[t]$视为F上的向量空间时是无限维的. 单项式$(1,t,t^2,\cdots)$构成一个基，用这个基可以如在第十章(2.8)中一样将$F[t]$等同于无限F-向量空间Z:
$$Z=\{(a_0,a_1,a_2,\cdots)\mid a_i\in F \text{ 并且仅有有限多个 } a_i \text{ 非零}\}.$$
在$F[t]$上用t乘对应于移位算子T:
$$(a_0,a_1,a_2,\cdots)\rightsquigarrow(0,a_0,a_1,a_2,\cdots).$$
这样，在同构下秩为1的自由$F[t]$-模对应于空间Z的位移算子.

现在我们开始应用到线性算子. 给定F上向量空间V的线性算子T，可以将V也视为$F[t]$-模. 假定V作为向量空间是有限维的，设为n维. 则它作为模当然是有限生成的，因此它有表现矩阵. 因为有两个矩阵可用，这里有搞混淆的危险：模V的表现矩阵和线性算子T的矩阵. 表现矩阵是元素为多项式的$r\times s$矩阵，其中r是模的选定的生成元的个数而s是关系的个数. 另一方面，线性算子的矩阵是$n\times n$标量矩阵，其中n是V作为向量空间的维数. 两个矩阵都含有描述模和线性算子所必需的信息.

将V视为$F[t]$-模，可以应用定理(6.13)得到V是循环子模的直和的结论，设
$$V=W_1\oplus\cdots\oplus W_k,$$

477

其中W_i同构于$F[t]/(p_i^{e_i})$，$p_i(t)$是$F[t]$的既约多项式. 因为假设V是有限维的，所以不存在自由直和项.

我们有两项任务：对于线性算子T解释直和分解的意义以及当模是循环模时描述线性算

子. 当选取适当的基时，直和分解给出了一个 T 的矩阵的块分解，这一点并不令人感到意外. 其原因是因为 W_i 是 $F[t]$-子模，子空间 W_i 中的每一个都是 T-不变的. 乘上 t 将 W_i 变到它自己，而 t 在 V 上作为线性算子 T 作用. 对子空间 W_i 选取基 $\mathbf{B}_i$，则 T 关于基 $\mathbf{B}=(\mathbf{B}_1,\cdots,\mathbf{B}_k)$ 的矩阵具有所希望的分块形式[第四章(3.8)].

其次，设 W 是循环 $F[t]$-模. 则 W 作为模由单独一个元素 w 生成. 换言之，W 的每个元素可以写为

$$g(t)w=b_rt^rw+\cdots+b_1tw+b_0w$$

的形式，其中 $g(t)=b_rt^r+\cdots+b_1t+b_0\in F[t]$. 这表明元素 w，tw，t^2w，…张成向量空间 W. 用线性算子的语言表述为 W 是由向量 w，$T(w)$，$T^2(w)$，…张成的.

$F[t]$-模与对应的线性算子的性质之间的各种联系总结如下表：

【7.6】词典

用 t 乘	T 的作用
秩为 1 的自由模	移位算子
由 v 生成的循环模	由 v，Tv，T^2v，…张成的空间
子模	T-不变子空间
子模的直和	T-不变子空间的直和
$F[t]$-模	线性算子 T

现在计算向量空间上对应于循环 $F[t]$-模的一个线性算子 T 的矩阵. 由于 $F[t]$的每个理想是主理想，这样的模将同构于形如

【7.7】
$$W=F[t]/(f)$$

的模，其中 $f(t)=t^n+a_{n-1}t^{n-1}+\cdots+a_1t+a_0$ 是 $F[t]$中的一个多项式. 用符号 w_0 表示 1 在 W 中的剩余. 这是我们选定的模的生成元. 于是关系 $fw_0=0$ 成立，并且 f 生成关系模.

元素 w_0，tw_0，…，$t^{n-1}w_0$ 构成 $F[t]/(f)$的基[见第十章(5.7)]. 我们用 $w_i=t^iw_0$ 表示这个基. 则有

$$tw_0=w_1,\quad tw_1=w_2,\quad\cdots,\quad tw_{n-2}=w_{n-1},$$

以及 $fw_0=0$. 用其他关系重写最后一个关系可以确定 t 在 w_{n-1}上的作用：

$$(t^n+a_{n-1}t^{n-1}+\cdots+a_1t+a_0)w_0=tw_{n-1}+a_{n-1}w_{n-1}+\cdots+a_1w_1+a_0w_0=0.$$

478

由于 T 的作用为用 t 乘，我们有

$$T(w_0)=w_1,\quad T(w_1)=w_2,\quad\cdots,\quad T(w_{n-2})=w_{n-1},$$

以及

$$T(w_{n-1})=-a_{n-1}w_{n-1}-\cdots-a_1w_1-a_0w_0.$$

这确定了 T 的矩阵，对不同的 n 值的表示如下：

【7.8】
$$[-a_0],\begin{bmatrix}0&-a_0\\1&-a_1\end{bmatrix},\begin{bmatrix}0&0&-a_0\\1&0&-a_1\\0&1&-a_2\end{bmatrix},\cdots,\begin{bmatrix}0&&&&-a_0\\1&0&&&-a_1\\&1&0&&\cdot\\&&\ddots&\ddots&\cdot\\&&&\ddots\ 0&\cdot\\&&&1&-a_{n-1}\end{bmatrix}$$

【7.9】定理 设 T 是域 F 上有限维向量空间 V 的线性算子. 存在 V 的一个基使得 T 关于这个基的矩阵由(7.8)型的分块构成.

线性算子矩阵的这样一个形式称为一个有理典范型. 它不是特别的漂亮, 但却是一个对任意域都可以得到的最好的形式.

例如, 模(6.4)是两个模的直和. 其有理典范型是

【7.10】
$$\left[\begin{array}{cc|c} & -1 & \\ 1 & 2 & \\ \hline & & 2 \end{array}\right].$$

我们现在进一步仔细地考虑 F 是复数域的情形. $\mathbb{C}[t]$ 中的每个既约多项式都是线性的, $p(t)=t-\alpha$, 因而根据定理(6.12), 每个有限维 $\mathbb{C}[t]$-模是一个同构于形如

【7.11】
$$W=\mathbb{C}[t]/(t-\alpha)^n$$

的子模的直和. 像前面一样用 w_0 表示 1 在 W 中的剩余, 但这次选择 W 的另外一个基, 令 $w_i=(t-\alpha)^i w_0$. 则

$$(t-\alpha)w_0=w_1,\quad (t-\alpha)w_1=w_2,\quad \cdots,\quad (t-\alpha)w_{n-2}=w_{n-1},\quad (t-\alpha)w_{n-1}=0.$$

用 T 代替 t 并求解得到对 $i=0, \cdots, n-2$, 有

$$Tw_i=w_{i+1}+\alpha w_i,$$

而

479

$$Tw_{n-1}=\alpha w_{n-1}.$$

T 的矩阵具有形式

【7.12】
$$[\alpha],\quad \begin{bmatrix}\alpha & 0\\ 1 & \alpha\end{bmatrix},\quad \begin{bmatrix}\alpha & 0 & 0\\ 1 & \alpha & 0\\ 0 & 1 & \alpha\end{bmatrix},\quad \cdots,\quad \begin{bmatrix}\alpha & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & \alpha\end{bmatrix}.$$

这些矩阵称为若尔当块. 这样我们得到下列定理:

【7.13】定理 设 $T: V\longrightarrow V$ 是有限维复向量空间上的线性算子. 存在 V 的一个基使得 T 关于这个基的矩阵是由若尔当块组成的.

这样的一个矩阵称为具有若尔当型, 或者是一个若尔当矩阵. 注意它是下三角的, 因而对角元素是其特征值. 若尔当型比有理典范型漂亮得多.

不难证明每一个若尔当块有一个唯一的特征向量.

给定任意复方阵 A, 定理断言对某个可逆矩阵 P, PAP^{-1} 为若尔当型. 我们常将 PAP^{-1} 称为"A 的若尔当型". 它在块的置换之下是唯一的, 因为直和分解的项是唯一的, 虽然这一点还未加以证明.

模(6.14)的若尔当型是由两个若尔当块组成的:

【7.14】
$$\left[\begin{array}{cc|c} 1 & & \\ 1 & 1 & \\ \hline & & 2 \end{array}\right].$$

若尔当型的一个重要应用是一阶线性微分方程组

【7.15】
$$\frac{\mathrm{d}X}{\mathrm{d}t}=AX.$$

的显式解．如我们在第四章(7.11)所见，解这个方程的问题容易化简为解方程$\frac{\mathrm{d}X}{\mathrm{d}t}=\widetilde{A}X$，其中$\widetilde{A}=PAP^{-1}$是任意的相似矩阵．这样假定可以确定一个给定矩阵 A 的若尔当型$\widetilde{A}$，则只要解所得到的方程组就行了．接下来，这又化简为单独一个若尔当块的情形．在第四章(8.18)中计算了一个2×2若尔当块的例子．

一个任意的 $k\times k$ 若尔当块 A 的解可以通过计算矩阵指数确定．用 N 表示由将 $\alpha=0$ 代入(7.12)得到的矩阵．则 $N^k=0$．因此

$$\mathrm{e}^{Nt}=I+Nt/1!+\cdots+N^{k-1}t^{k-1}/(k-1)!.$$

这是一个下三角矩阵，其主对角线上为一条常数而主对角线下面的第 i 条对角线的元素都是 $t^i/i!$．因为 N 与 αI 可交换，

480

$$\mathrm{e}^{At}=\mathrm{e}^{\alpha t}\mathrm{e}^{Nt}=\mathrm{e}^{\alpha t}(I+Nt/1!+\cdots+N^{k-1}t^{k-1}/(k-1)!).$$

这样如果 A 是矩阵

$$\begin{bmatrix}3&&\\1&3&\\&1&3\end{bmatrix},$$

则

$$\mathrm{e}^{At}=\begin{bmatrix}\mathrm{e}^{3t}&&\\&\mathrm{e}^{3t}&\\&&\mathrm{e}^{3t}\end{bmatrix}\begin{bmatrix}1&&\\t&1&\\\frac{1}{2}t^2&t&1\end{bmatrix}=\begin{bmatrix}\mathrm{e}^{3t}&&\\t\mathrm{e}^{3t}&\mathrm{e}^{3t}&\\\frac{1}{2}t^2\mathrm{e}^{3t}&t\mathrm{e}^{3t}&\mathrm{e}^{3t}\end{bmatrix}.$$

第四章定理(8.14)告诉我们这个矩阵的列构成微分方程(7.15)的解空间的基．

计算一个给定矩阵的若尔当型需要求出其特征多项式 $p(t)$ 的根．如果根 $\alpha_1,\cdots,\alpha_n$ 互不相同，则若尔当型是对角的：

$$\begin{bmatrix}\alpha_1&&\\&\ddots&\\&&\alpha_n\end{bmatrix}$$

假设根 $\alpha_1=\alpha$ 是 $p(t)$ 的一个 r 重根．则若尔当矩阵以 α 为主对角元素的部分会有多种可能性．下面是当 r 不大时的一些可能性：

$$r=1:[\alpha];\quad r=2:\begin{bmatrix}\alpha&\\1&\alpha\end{bmatrix},\left[\begin{array}{c|c}\alpha&\\\hline&\alpha\end{array}\right];$$

$$r=3:\begin{bmatrix}\alpha&&\\1&\alpha&\\&1&\alpha\end{bmatrix},\left[\begin{array}{cc|c}\alpha&&\\1&\alpha&\\\hline&&\alpha\end{array}\right],\left[\begin{array}{c|c|c}\alpha&&\\\hline&\alpha&\\\hline&&\alpha\end{array}\right];$$

$$r=4:\begin{bmatrix}\alpha&&&\\1&\alpha&&\\&1&\alpha&\\&&1&\alpha\end{bmatrix},\ \left[\begin{array}{ccc|c}\alpha&&&\\1&\alpha&&\\&1&\alpha&\\\hline&&&\alpha\end{array}\right],\ \left[\begin{array}{cc|cc}\alpha&&&\\1&\alpha&&\\\hline&&\alpha&\\&&1&\alpha\end{array}\right],\ \left[\begin{array}{cc|c|c}\alpha&&&\\1&\alpha&&\\\hline&&\alpha&\\\hline&&&\alpha\end{array}\right],$$

$$\left[\begin{array}{c|c|c|c}\alpha&&&\\\hline&\alpha&&\\\hline&&\alpha&\\\hline&&&\alpha\end{array}\right].$$

481

通过计算与 T 相联系的某些算子的特征向量可以把它们区分开来．方程组

$$(A-\alpha I)x=0$$

的解空间是以 α 为特征值的特征向量空间．给定 A 和 α，这个方程组可以具体解出．如果 $r=4$，则上面所列五种情形中解空间的维数分别是 1，2，2，3，4，这是因为对每个块都有一个特征向量与之相伴．因而除了第二种与第三种情形外，这个维数是互不相同的．剩下的两种情形可由矩阵 $(A-\alpha I)^2$ 区别开来．它在第三种情形为零而在第二种情形不为零．

可以证明在所有情形中，算子 $(A-\alpha I)^{\nu}(\nu=1,2,\cdots,r/2)$ 的零点空间的维数区分了若尔当型．

第八节　多项式环上的自由模

随着环的复杂性的增加，环上模的结构也变得更加复杂．甚至要确定一个具体表现的模是否是自由的都是困难的．本节我们不加证明地描述刻画多项式环上自由模的定理．这个定理是在 1976 年由奎伦(Quillen)和苏斯林(Suslin)证明的．

设 $R=\mathbb{C}[x_1,\cdots,x_k]$ 是 k 个变量的多项式环，并设 V 是有限生成 R-模．我们选定模的一个表现矩阵 A．A 的元素是多项式 $a_{ij}(x)$，且如果 A 是 $m\times n$ 矩阵，则 V 同构于 A 在 R-向量上乘积的余核 R^m/AR^n．可以让矩阵元素在 $\mathbb{C}^k$ 的任意点 $p=(p_1,\cdots,p_k)$ 取值而得到 i，j-元是 $a_{ij}(p)$ 的复矩阵 $A(p)$．

【8.1】定理　*设 V 是多项式环 $\mathbb{C}[x_1,\cdots,x_k]$ 上的有限生成模，并设 A 是 V 的一个 $m\times n$ 表现矩阵．用 $A(p)$ 表示 A 在点 $p\in\mathbb{C}^k$ 的取值．则 V 是秩为 r 的自由模当且仅当对每个点 p，$A(p)$ 的秩为 $m-r$．*

现在我们还没有证明这个定理所需要的背景知识．然而，可以很容易地看到如何用它来确定一个给定的模是否自由．例如，考虑两个变量的多项式环：$R=\mathbb{C}[x,y]$．设 V 是由 4×2 矩阵

【8.2】
$$A=\begin{bmatrix}1&x\\y&x+3\\x&y\\x^2&y^2\end{bmatrix}$$

482

表现的模．则 V 有四个生成元和两个关系．设 p 是一个点 $(a,b)\in\mathbb{C}^2$．矩阵 $A(p)$ 的两个列为

$$v_1=(1,b,a,a^2)^t,\quad v_2=(a,a+3,b,b^2)^t.$$

不难证明对于 a，b 的每一个选择，这两个向量是线性无关的，由此得到对每个点 (a,b)，$A(p)$ 的秩为 2．要使这两个向量相关则必需满足 $v_2=cv_1$，反之亦然．于是第一个坐标表明 $v_2=av_1$，

因此

【8.3】 $$a+3=ab,\quad b=a^2,\quad b^2=a^3.$$

这几个方程没有公共解．由定理(8.1)，V 是秩为 2 的自由模．

我们可以通过考虑由复矩阵 $A(p)$ 表现的向量空间 $V_p=\mathbb{C}^m/A(p)\mathbb{C}^n$ 而得到对这个定理的一个直观理解．自然可将这个向量空间理解为一种"模 V 在 p 点的取值，"可以证明 V_p 在本质上与表现矩阵的选择是无关的．因而可用模 V 使每个点 $p\in\mathbb{C}^k$ 与一个向量空间 V_p 相伴．如果想象在移动点 p 时，假定向量空间 V_p 的维数不跳跃的话，则它将以连续的方式变化．这是由于表现 V_p 的矩阵 $A(p)$ 连续地依赖于 p．由一个拓扑空间参数化的固定维数的向量空间簇称为向量丛．模是自由的当且仅当向量空间簇 V_p 构成一个向量丛．

我认为对数学家来说通常的变形过于保守．

Jean-Louis Verdier

练　习

第一节　模的定义

1. 设 R 是一个环，看作 R-模．确定所有模同态 $\varphi:R\longrightarrow R$．
2. 设 W 是 R-模 V 的子模．证明 W 中一个元的加法逆属于 W．
3. 设 $\varphi:V\longrightarrow W$ 是环 R 上模的同态，并设 V'，W' 分别是 V，W 的子模．证明 $\varphi(V')$ 是 W 的子模而 $\varphi^{-1}(W')$ 是 V 的子模．
4. (a) 设 V 是阿贝尔群．证明如果 V 有一个以其给定的合成法则为加法的$\mathbb{Q}$-模结构，则这个结构是唯一确定的．
   (b) 证明有限阿贝尔群不能有$\mathbb{Q}$-模结构．
5. 设 $R=\mathbb{Z}[\alpha]$，其中 α 是一个代数整数．证明对任意整数 m，R/mR 是有限的，并求其阶． 483
6. 一个模如果不是零模且没有真子模，则称为单模．
   (a) 证明任意单模同构于 R/M，其中 M 是一个极大理想．
   (b) 证明舒尔引理：设 $\varphi:S\longrightarrow S'$ 是单模的同态．则 φ 或者为零，或者是一个同构．
7. R-模 V 的零化子是集合 $I=\{r\in R\mid rV=0\}$．
   (a) 证明 I 是 R 的理想．
   (b) $\mathbb{Z}$-模$\mathbb{Z}/(2)\times\mathbb{Z}/(3)\times\mathbb{Z}/(4)$的零化子是什么？$\mathbb{Z}$-模$\mathbb{Z}$的零化子又是什么？
8. 设 R 是环而 V 是 R-模．设 E 是 V 的自同态的集合，也就是 V 到自身的同态的集合．证明 E 是个非交换环，乘法为函数的合成而加法由$[\varphi+\psi](m)=\varphi(m)+\psi(m)$定义．
9. 证明一个单模的自同态环是域．
10. 确定 R-模的自同态环(a)R 和(b)R/I，其中 I 是一个理想．
11. 设 $W\subset V\subset U$ 是 R-模．
    (a) 描述与三个商模 U/W，U/V 和 V/W 相关的自然同态．
    (b) 证明第三同构定理：$U/V\approx(U/W)/(V/W)$．
12. 设 V，W 是模 U 的子模．
    (a) 证明 $V\cap W$ 和 $V+W$ 是子模．
    (b) 证明第二同构定理：$(V+W)/W$ 与 $V/(V\cap W)$同构．
13. 设 V 是如在(1.1)中所定义的 R-模．如果环 R 不交换，则定义 $vr=rv$ 是不行的．对此作出解释．

第二节 矩阵、自由模和基

1. 设 $R=\mathbb{C}[x,y]$，并设 M 是 R 中由两个元素 (x, y) 生成的理想. 证明或推翻：M 是自由 R-模.
2. 设 A 是系数属于一个环 R 的 $n\times n$ 矩阵，设 $\varphi:R^n \longrightarrow R^n$ 是用 A 左乘，并设 $d=\det A$. 证明或推翻：φ 的象等于 dR^n.
3. 设 I 是环 R 的理想. 证明或推翻：若 R/I 是自由 R-模，则 $I=0$.
4. 设 R 是环，并设 V 是秩有限的自由 R-模. 证明或推翻：
   (a) 每一个生成元集含有一个基.
   (b) 每一个线性无关的集合可以拓广为一个基.
5. 设 I 是环 R 的理想. 证明 I 是自由 R-模当且仅当它是由一个不是 R 中的零因子的元素 α 生成的主理想.
6. 证明使得有限生成 R-模都是自由模的环 R 是一个域或零环.
7. 设 A 是自由模间的同态 $\varphi:\mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ 的矩阵.
   (a) 证明 φ 是单射当且仅当 A 的秩为 n.
   (b) 证明 φ 是满射当且仅当 A 的 $m\times m$ 阶子式的行列式的最大公因数为 1.

484

8. 证明第二节给出的自由阿贝尔群的定义与第六章第八节给出的定义是一致的.

第三节 恒等式的不变性原理

1. 在每一种情形，确定恒等式的不变性原理是否能使结论从复数搬到任意交换环.
   (a) 矩阵乘法的结合律
   (b) 凯莱-哈密顿定理
   (c) 克莱姆法则
   (d) 多项式微分的乘法法则、除法法则和链式法则
   (e) n 次多项式最多有 n 个根这一事实
   (f) 多项式的泰勒展开式
2. 恒等式的不变性原理是否表明当矩阵的元素属于非交换环 R 时 $\det AB=\det A\,\det B$ 成立？
3. 在某些情形，只对实数验证恒等式会是方便的. 这足够吗？
4. 设 R 是环，并设 A 是 $SO_3(R)$ 中的一个 $3\times 3R$-矩阵，即满足 $A^tA=I$ 且 $\det A=1$. 恒等式的不变性原理是否表明 A 在 R^3 中有一个特征值为 1 的特征向量？

第四节 整数矩阵的对角化

1. 通过整数行和列变换化简下列每个矩阵.

$$\text{(a)}\begin{bmatrix}3&1\\-1&2\end{bmatrix}\quad\text{(b)}\begin{bmatrix}1&2&3\\4&5&6\end{bmatrix}\quad\text{(c)}\begin{bmatrix}3&1&-4\\2&-3&1\\-4&6&-2\end{bmatrix}$$

   (d) 在第一种情形，设 $V=\mathbb{Z}^2$ 并设 $L=AV$. 画出子格 L，并求 V 和 L 的可公度的基.
2. 设 A 是元素属于多项式环 $F[t]$ 的矩阵，并设 A' 是由 A 通过多项式行和列变换得到的矩阵. 将 $\det A$ 与 $\det A'$ 联系起来.
3. 确定对角化矩阵 $A=\begin{bmatrix}4&7&2\\2&4&6\end{bmatrix}$ 的整数矩阵 P^{-1}，Q.
4. 设 d_1，d_2，…是定理(4.3)中提到的整数.
   (a) 证明 d_1 是 A 的元素 a_{ij} 的最大公因数.
   (b) 证明 d_1d_2 是 A 的 2×2 子式的行列式的最大公因数.
   (c) 对任意 i 叙述并证明(a)和(b)对 d_i 的拓广.

5. 当 $A=\begin{bmatrix}4&7&2\\2&4&6\end{bmatrix}$时，求方程组 $AX=0$ 的所有整数解.

6. 求$\mathbb{Z}^3$ 的下列子模的基.

   (a) 由(1, 0, −1), (2, −3, 1), (0, 3, 1), (3, 1, 5)生成的模.

   (b) 方程组 $x+2y+3z=0$, $x+4y+9z=0$ 的解的模.

7. 证明两个矩阵$\begin{bmatrix}1&1\\&1\end{bmatrix}$和$\begin{bmatrix}&-1\\1&\end{bmatrix}$生成行列式为 1 的整数矩阵群 $SL_2(\mathbb{Z})$.

485

8. 证明群 $SL_n(\mathbb{Z})$由第一类型的初等整数矩阵生成.

9. 设 α, β, γ 是复数，并设 $A=\{\ell\alpha+m\beta+n\gamma \mid \ell, m, n\in\mathbb{Z}\}$是它们生成的$\mathbb{C}^+$ 的子群. 在什么条件下 A 是$\mathbb{C}$ 中的格?

10. 设 $\varphi:\mathbb{Z}^k\longrightarrow\mathbb{Z}^k$ 是由乘一个整数矩阵 A 得到的同态. 证明 φ 的象的指标有限当且仅当 A 是非奇异的，并且这时其指标等于 $|\det A|$.

11. (a) 设 $A=(a_1, \cdots, a_n)^t$ 为整数列向量. 用行约化证明存在矩阵 $P\in GL_n(\mathbb{Z})$使得 $PA=(d, 0, \cdots, 0)^t$，其中 d 是 a_1, …, a_n 的最大公因数.

    (b) 证明如果 $d=1$，则 A 是一个矩阵 $M\in SL_n(\mathbb{Z})$的第一列.

第五节　模的生成元与关系

1. 在每一情形，确定具有给定表现矩阵的阿贝尔群:

$$\begin{bmatrix}2\\1\end{bmatrix},\begin{bmatrix}0\\5\end{bmatrix},\begin{bmatrix}2&0&0\end{bmatrix},\begin{bmatrix}1&\\1&1\end{bmatrix},\begin{bmatrix}1&0\\0&1\\0&0\end{bmatrix},\begin{bmatrix}2&3\\1&2\end{bmatrix},\begin{bmatrix}2&4\\1&4\end{bmatrix},\begin{bmatrix}4&6\\2&3\end{bmatrix}.$$

2. 求环 R 及 R 的理想 I 使之不是有限生成的.

3. 证明因子分解的存在性在诺特整环中是成立的.

4. 设$V\subset\mathbb{C}^n$ 是一个多项式的无限集合 f_1, f_2, …的零点的轨迹. 证明存在这些多项式的一个有限子集，其零点定义同样的轨迹.

5. 设 S 是$\mathbb{C}^n$ 的子集. 证明存在多项式的有限集合(f_1, f_2, …, f_k)，使得任意在 S 上恒为零的多项式是这个集合的一个系数为多项式的线性组合.

6. 求$\mathbb{Z}[\delta]$中理想(2, $1+\delta$)的表现矩阵，其中 $\delta=\sqrt{-5}$.

*7. 设 S 是环 $R=\mathbb{C}[t]$的子环，包含$\mathbb{C}$ 且不等于$\mathbb{C}$. 证明 R 是有限生成 S-模.

8. 设 A 是模 V 关于生成元集(v_1, …, v_m)的表现矩阵. 设(w_1, …, w_r)是 V 的另一个用生成元表出的元素的集合，设这些生成元为 $w_i=\sum p_{ij}v_j$, $p_{ij}\in R$. 令 $P=(p_{ij})$. 证明分块矩阵$\left[\begin{array}{c|c}A&-P\\\hline 0&I\end{array}\right]$是模 V 关于生成元集(v_1, …, v_m; w_1, …, w_r)的一个表现矩阵.

*9. 用前面问题的记号，假设(w_1, …, w_r)也是 V 的一个生成元集，并设 B 是 V 关于这个生成元集的表现矩阵. 设 $v_i=\sum q_{ij}w_j$ 是生成元 v_i 用 w_j 表出的表达式.

   (a) 证明分块矩阵 $M=\left[\begin{array}{c|c|c|c}A&-P&I&0\\\hline 0&I&-Q&B\end{array}\right]$ 关于生成元集(v_1, …, v_m; w_1, …, w_r)表现模 V.

   (b) 证明通过一系列形如(5.12)的变换 M 可以化为 A 和也可以化为 B.

10. 用 9 证明可以通过一系列变换(5.12)及其逆将模的任一个表现矩阵化为另一个.

486

第六节 阿贝尔群的结构定理

1. 求同构于由矩阵$\begin{bmatrix}2&2&2\\2&2&0\\2&0&2\end{bmatrix}$表现的阿贝尔群的循环群的直和.

2. 将由x，y生成且满足关系$3x+4y=0$的群写成循环群的直和.

3. 当V是由x，y，z生成的群且分别满足下列关系时，求出其同构的循环群的直积.

 (a) $3x+2y+8z=0$，$2x+4z=0$

 (b) $x+y=0$，$2x=0$，$4x+2z=0$，$4x+2y+2z=0$

 (c) $2x+y=0$，$x-y+3z=0$

 (d) $2x-4y=0$，$2x+2y+z=0$

 (e) $7x+5y+2z=0$，$3x+3y=0$，$13x+11y+2z=0$

4. 确定400阶阿贝尔群的同构类的个数.

5. 在下面每一个环上对有限生成模分类.

 (a) $\mathbb{Z}/(4)$ (b) $\mathbb{Z}/(6)$ (c) $\mathbb{Z}/n\mathbb{Z}$

6. 设R是环，并设V是一个R-模，由一个对角$m\times n$矩阵A表现：$V\approx R^m/AR^n$. 设$(v_1, \cdots, v_m)$是V对应的生成元，并设d_i是A的对角元. 证明V同构于模$R/(d_i)$的直积.

7. 设V是由元素v_1，v_2生成且满足关系$(1+i)v_1+(2-i)v_2=0$，$3v_1+5iv_2=0$的$\mathbb{Z}[i]$-模. 把这个模写为循环模的直和.

8. 设$W_1, \cdots, W_k$是R-模V的子模且满足$V=\sum W_i$. 假设$W_1\cap W_2=0$，$(W_1+W_2)\cap W_3=0$，…，$(W_1+W_2+\cdots+W_{k-1})\cap W_k=0$. 证明$V$是模$W_1, \cdots, W_k$的直和.

9. 证明下列结论.

 (a) $\mathbb{Z}/(p^e)$中阶整除p^ν的元素的个数当$\nu\leqslant e$时为p^ν，而当$\nu\geqslant e$时为p^e.

 (b) 设$W_1, \cdots, W_k$是有限阿贝尔群，并设u_j表示W_j中阶整除一个给定整数q的元素的个数. 则积群$V=W_1\times\cdots\times W_k$中阶整除$q$的元素的个数为$u_1\cdots u_k$.

 (c) 用上面的记号，假定W_j是素数幂$d_j=p^{e_j}$阶循环群. 设r_1是等于给定素数p的d_j的个数，设r_2是等于p^2的d_j的个数，等等. 则V中阶整除p^ν的元素的个数为p^{s_ν}，其中$s_1=r_1+\cdots+r_k$，$s_2=r_1+2r_2+\cdots+2r_k$，$s_3=r_1+2r_2+3r_3+\cdots+3r_k$，等等.

 (d) 定理(6.9).

第七节 对线性算子的应用

487

1. 设T是矩阵为$\begin{bmatrix}2&1\\0&1\end{bmatrix}$的线性算子. 对应的$\mathbb{C}[t]$-模是否是循环模?

2. 求矩阵$\begin{bmatrix}1&1&0\\0&1&0\\0&1&1\end{bmatrix}$的若尔当型.

3. 证明$\begin{bmatrix}1&1&1\\-1&-1&-1\\1&1&1\end{bmatrix}$为幂等矩阵，并求其若尔当型.

4. 设V是一个5维复向量空间，并设T是V上特征多项式为$(t-\alpha)^5$的线性算子. 假设算子$T-\alpha I$的秩为2. T可能的若尔当型是什么?

5. 对特征多项式为$(t+2)^2(t-5)^3$的矩阵求出其所有可能的若尔当型.

6. 对特征多项式为$(t-2)^2(t-5)^3$的矩阵，如果其特征值为2的特征向量空间是一维的，而特征值为5的特征向量空间是二维的，那么它的若尔当型是什么？
7. (a) 证明一个若尔当块有一个一维的特征向量空间.
   (b) 反过来，证明如果一个复矩阵A的特征向量是单独一个向量的倍数，则A的若尔当型由一个若尔当块组成.
8. 求其若尔当型由一个块组成的线性算子的所有不变子空间.
9. 对下列每一情形，当矩阵A是给定的若尔当块时，解微分方程$dX/dt=AX$：

$$\text{(a)}\begin{bmatrix}2&\\1&2\end{bmatrix}\quad\text{(b)}\begin{bmatrix}0&0\\1&0\end{bmatrix}\quad\text{(c)}\begin{bmatrix}1&&\\1&1&\\&1&1\end{bmatrix}$$

10. 当A为(a)矩阵(7.14)，(b)矩阵(7.10)，(c)问题2的矩阵，(d)问题3的矩阵时，解微分方程$dX/dt=AX$.
11. 证明或推翻：两个复$n\times n$矩阵相似当且仅当它们有相同的若尔当型.
12. 证明每个复$n\times n$矩阵与一个形如$D+N$的矩阵相似，其中D是对角的，N是幂零的，并且$DN=ND$.
13. 设$R=F[x]$是域F上的一元多项式环，并设V是一个由满足关系$(x^3+3x+2)v=0$的元素v生成的R-模. 选择一个V的作为F-向量空间的基，并求用t乘所定义的算子关于这个基的矩阵.
14. 设V是一个$F[t]$-模，且设$\mathbf{B}=(v_1, \cdots, v_n)$是$V$作为$F$-向量空间的基. 设$B$是$T$关于这个基的矩阵. 证明$A=tI-B$是模的表现矩阵.
15. 设$p(t)$是域F上的多项式. 证明存在元素属于F的$n\times n$矩阵，其特征多项式为$p(t)$.
16. 证明或推翻：满足$A^2=A$的一个复矩阵A是可对角化的.
17. 设A是复$n\times n$矩阵且对某个k有$A^k=I$，证明A的若尔当型是对角的.
18. 证明凯莱-哈密顿定理：如果$p(t)$是$n\times n$矩阵A的特征多项式，则$p(A)=0$.

488

19. 复向量空间V的线性算子T的极小多项式$m(t)$是使$m(T)=0$的最低次数的多项式.
   (a) 证明极小多项式整除特征多项式.
   (b) 证明特征多项式$p(t)$的每个根都是极小多项式$m(t)$的根.
   (c) 证明T可对角化当且仅当$m(t)$没有重根.
20. 对极小多项式为$x^2(x-1)^3$的8×8矩阵求出其所有可能的若尔当型.
21. 证明或推翻：一个复矩阵A与其转置相似.
22. 去掉模作为向量空间是有限维的假设，对有限生成$F[t]$-模上的线性算子进行分类.
23. 证明$(A-\alpha I)^k$的秩区分所有的若尔当型，因而若尔当型仅与算子有关而与基无关.
24. 证明下列概念是等价的：
   (a) R-模，其中$R=\mathbb{Z}[i]$；
   (b) 阿贝尔群V连同一个使$\varphi\circ\varphi=-$恒等映射的同态$\varphi: V\longrightarrow V$.
25. 设$F=\mathbb{F}_p$. 对什么素数p加法群F^1具有$\mathbb{Z}[i]$-模结构？F^2的情形又怎样呢？
26. 对$\mathbb{C}[\epsilon]$上的有限生成模分类，其中$\epsilon^2=0$.

第八节 多项式环上的自由模

1. 确定$\mathbb{C}[x, y]$上由下列矩阵表现的模是否自由.

$$\text{(a)}\begin{bmatrix}x^2+1&x\\x^2y+x+y&xy+1\end{bmatrix}\quad\text{(b)}\begin{bmatrix}xy-1\\x^2-y^2\\y\end{bmatrix}\quad\text{(c)}\begin{bmatrix}x-1&x\\y&y+1\\x&y\\x^2&2y\end{bmatrix}$$

2. 通过写出一个基证明由(8.2)表现的模是自由的.
3. 按一元多项式环的模型，用带有附加结构的实向量空间的语言描述环$\mathbb{C}[x,y]$上的模.
4. 设R是环而V是R-模. 设I是R的理想，并设IV是有限和$\sum s_i v_i$的集合，其中$s_i \in I$而$v_i \in V$.
   (a) 说明如何将V/IV做成R/I-模.
   (b) 设A是V的表现矩阵，并用$\overline{A}$记它在R/I的剩余. 证明$\overline{A}$是V/IV的表现矩阵.
   (c) 说明为什么文中定义的模V_p在本质上与表现矩阵无关.
*5. 用第五节的练习9证明苏斯林–奎伦定理较容易的那一半：如果V自由，则$A(p)$的秩为常数.
6. 设$R=\mathbb{Z}[\sqrt{-5}]$,并设V是由矩阵$A=\begin{bmatrix}2\\1+\delta\end{bmatrix}$表现的模.
   (a) 证明对R的每个素理想P有A的剩余的秩为1.
   (b) 证明V不是自由的.

489

杂题

1. 设G是个格群而g是G中的旋转. 设$\overline{g}$是在点群$\overline{G}$中相伴的元素. 证明存在$\mathbb{R}^2$的基(不一定是个标准正交基)使得$\overline{g}$关于这个基的矩阵属于$GL_2(\mathbb{Z})$.
*2. (a) 设α是复数并设$\mathbb{Z}[\alpha]$是$\mathbb{C}$中由α生成的子环. 证明α是代数整数当且仅当$\mathbb{Z}[\alpha]$是有限生成阿贝尔群.
   (b) 证明如果α，β是代数整数，则它们生成的$\mathbb{C}$的子环$\mathbb{Z}[\alpha,\beta]$是有限生成阿贝尔群.
   (c) 证明代数整数构成$\mathbb{C}$的子环.
*3. *皮克定理*：设Δ是由其项点为整格点的多边形所界定的平面区域. 设I是在Δ内部的格点的集合而B是在Δ边界上的格点的集合. 如果p是格点，设$r(p)$表示p处Δ的对角的2π的分数. 于是如果$p\notin\Delta$，则$r(p)=0$;如果p是Δ的内点，则$r(p)=1$；如果p在一个边上，则$r(p)=\frac{1}{2}$，等等.
   (a) 证明Δ的面积为$\sum_p r(p)$.
   (b) 证明如果Δ有一条单连通边界曲线，则面积为$|I|+\frac{1}{2}(|B|-2)$.
4. 证明整数正交群$O_n(\mathbb{Z})$是有限群.
*5. 考虑作为内积空间的列向量空间$V=\mathbb{R}^k$，具有通常的点积$(v\cdot w)=v^t w$. 设L是V中的一个格，定义$L^*=\{w \mid 对所有 v\in L 有(v\cdot w)\in\mathbb{Z}\}$.
   (a) 证明L^*是一个格.
   (b) 设$\boldsymbol{B}=(v_1,\cdots,v_k)$是$L$的一个格基，并设$P=[\boldsymbol{B}]^{-1}$是将$V$的这个基与标准基$\boldsymbol{E}$相联系的矩阵. 点积关于基$\boldsymbol{B}$的矩阵$A$是什么?
   (c) 证明P的列构成L^*的一个格基.
   (d) 证明如果A是整数矩阵，则$L\subset L^*$，且$[L^*:L]=|\det A|$.
6. 设V是具有可数无限基$\{v_1,v_2,v_3,\cdots\}$的实向量空间，并设E是V上线性算子的环.
   (a) 哪些无穷矩阵代表V上的线性算子?
   (b) 描述如何用两个线性算子的矩阵描述它们合成的矩阵.
   (c) 考虑由法则
$$T(v_{2n})=v_n,\quad T(v_{2n-1})=0,\quad T'(v_{2n})=0, T'(v_{2n-1})=v_n,\quad n=1,2,3,\cdots$$
   定义的线性算子T，T'. 写出它们的矩阵.
   (d) 可将$E^1=E$视为环E上的模，标量乘法在向量的左边. 证明$\{T,T'\}$是E^1作为E-模的基.
   (e) 证明所有自由E-模$E^k(k=1,2,3,\cdots)$都是同构的.

7. 证明群$\mathbb{Q}^+/\mathbb{Z}^+$不是循环群的无限直和.

8. 证明有理数加法群$\mathbb{Q}^+$不是两个真子群的直和.

9. 证明有理数乘法群$\mathbb{Q}^\times$同构于一个2阶循环群和一个有可数多个生成元的自由阿贝尔群的直和.

490

10. 证明两个可对角化的矩阵可同时对角化，即存在可逆矩阵P使得PAP^{-1}和PBP^{-1}都是对角的当且仅当$AB=BA$.

*11. 设A是有限阿贝尔群，并设$\varphi:A\longrightarrow\mathbb{C}^\times$是一个非平凡的同态(对所有$x$，都有$\varphi(x)=1$). 证明$\sum_{a\in A}\varphi(a)=0$.

12. 设A是系数属于环R的$m\times n$矩阵，并设$\varphi:R^n\longrightarrow R^m$是用$A$左乘. 证明下列结论等价：

(a) φ是满射；

(b) A的$m\times m$子式的行列式生成单位理想；

(c) A有右逆，即系数属于R的矩阵B使得$AB=I$.

*13. 设$(v_1,\cdots,v_m)$是R-模V的生成元，J是R的一个理想. 定义JV为积$av(a\in J, v\in V)$的所有有限和的集合.

(a) 证明如果$JV=V$，则存在元素属于J的$n\times n$矩阵A使得$(v_1,\cdots,v_m)(I-A)=0$.

(b) 用(a)的记号，证明$\det(I-A)=1+\alpha$，其中$\alpha\in J$，并且$\det(I-A)$零化V.

(c) R-模V称为忠实的，如果对$r\in R$，$rV=0$蕴涵$r=0$. 证明中山引理：设V是有限生成的忠实R-模，并设J是R的理想. 如果$JV=V$，则$J=R$.

(d) 设V是有限生成R-模. 证明如果对所有极大理想M有$MV=V$，则$V=0$.

*14. 可用一对t的复多项式$x(t)$，$y(t)$通过令$t\rightsquigarrow(x(t),y(t))$来定义$\mathbb{C}^2$中复路. 通过令$f(x,y)\rightsquigarrow f(x(t),y(t))$也定义一个同态$\varphi:\mathbb{C}[x,y]\longrightarrow\mathbb{C}[t]$. 这个练习分析路与同态间的关系. 我们排除$(x(t),y(t))$都是常数的平凡情形.

(a) 设S表示φ的象. 证明S同构于商$\mathbb{C}[x,y]/(f)$，其中$f(x,y)$为一个既约多项式.

(b) 证明t是一个系数属于S的首一多项式的根.

(c) 设V表示f在$\mathbb{C}^2$中的零点的簇. 证明对任意点$(x_0,y_0)\in V$，存在$t_0\in\mathbb{C}$使得$(x_0,y_0)=(x(t_0),y(t_0))$.

491

第十三章　域

我们的困难不在于证明，

而在于学习证明什么.

Emil Artin

第一节　域的例子

域理论的大部分与其中一个包含在另一个之中的一对域 $F\subset K$ 有关. 与群论形成对照的是，在群论中子群起着重要的作用，而我们通常将 K 视为 F 的扩张；即把 F 看作是基本域而 K 与它相关. F 的扩域是包含 F 为其子域的域.

下面是三个最重要的域类.

【1.1】数域　数域 K 是$\mathbb{C}$的一个子域.

$\mathbb{C}$的任意子域包含 1，因而它包含有理数域$\mathbb{Q}$. 因而一个数域是$\mathbb{Q}$的扩域. 最常用到的数域是其所有元素都是代数数(见第十章第一节)的代数数域. 我们在第十一章学习了二次数域.

【1.2】有限域　有有限多个元素的域称为一个有限域.

设 K 是有限域，则唯一的同态 $\varphi:\mathbb{Z}\longrightarrow K$ 的核是素理想，由于$\mathbb{Z}$是无限的而 K 是有限的，因此核不为零. 因而它由一个素整数 p 生成. φ 的象与商$\mathbb{Z}/(p)=\mathbb{F}_p$同构. 所以 K 包含一个与素域$\mathbb{F}_p$同构的子域，因而可以将它看作是这个素域的一个扩域. 我们将在第六节描述所有的有限域.

492

【1.3】函数域　有理函数域 $F=\mathbb{C}(x)$的某些扩张称为函数域.

函数域在解析函数论和代数几何中起着重要的作用. 由于我们以前没有见到过，在这里对它们做个简要的描述. 函数域可用一个二元既约多项式，如 $f(x, y)\in\mathbb{C}[x, y]$来定义. 多项式 $f(x, y)=y^2-x^3+x$ 是一个很好的例子. 给定一个这样的多项式 f，我们可以解析地研究方程

【1.4】
$$f(x,y)=0,$$

如在微积分中所学的那样，用它"隐式地"将 y 定义为 x 的函数 $y(x)$. 在我们的例子中，这样定义的函数是 $y=\sqrt{x^3-x}$. 这不是一个单值函数；它在只相差一个符号的情况下被确定，但真正的困难不在于此. 对这样的函数一般不会有一个显式的表达式，但由定义，它满足方程(1.4)，即

【1.5】
$$f(x,y(x))=0.$$

另一方面，也可以从代数的角度来研究这个方程. 我们把 $f(x, y)$解释为一个 y 的多项式，其系数是 x 的多项式. 设 F 表示 x 的有理函数域$\mathbb{C}(x)$. 如果 f 不是 x 单独一个变量的多项式，则由于它在$\mathbb{C}[x, y]$中既约，它也是 $F[y]$上的一个既约元[第十一章(3.9)]. 因此在 $F[y]$中由 f 生成的理想是极大理想[第十一章(1.6)]，并且$F[y]/(f)=K$ 是 F 的扩域.

分析和代数是联系着的，因为隐式定义的函数 $y(x)$ 及 y 在 $F[y]/(f)$ 中的剩余 $\bar{y}$ 都满足方程 $f(x, y)=0$. y 的剩余，事实上 K 的所有元素都可以用这种方式解释为变量 x 的函数. 因为这一点，这样的域称为函数域. 我们将在第七节讨论函数域.

第二节　代数元与超越元

设 K 是域 F 的一个扩域，并设 α 是 K 的元素. 与代数数的定义(第十章第一节)类似，元素 α 称为在 F 上是代数的，如果 α 是一个系数属于 F 的某个非零多项式的根. 由于系数取自一个域，因而可以假定多项式是首一的，比如

【2.1】
$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad \text{其中 } a_i \in F.$$

一个元素 α 称为在 F 上是超越的，如果它在 F 上不是代数的，即它不是任意这样多项式的根.

注意代数的和超越的这两个性质依赖于给定的域 F. 例如，复数 $2\pi i$ 在实数域上是代数的但在有理数域上是超越的. 而且一个域 K 中的每个元素 α 在 K 上是代数的，因为它是多项式 $x-\alpha$ 的根，其系数属于 K.

493

元素 α 的这两种可能性可以用代入同态

【2.2】
$$\varphi: F[x] \longrightarrow K, \quad \text{它使得 } f(x) \rightsquigarrow f(\alpha)$$

来描述. 如果 φ 是单射，则元素 α 在 F 上是超越的，而在其他情形，即如果 φ 的核不等于零，则它在 F 上是代数的.

假设 α 在 F 上是代数的. 由于 $F[x]$ 是主理想整环，$\ker\varphi$ 由单独一个元素 $f(x)$ 生成，即以 α 为根的次数最低的首一多项式. 由于 K 是域，我们知道 $f(x)$ 必为既约多项式，事实上它是这个理想中仅有的首一既约多项式. 理想中的每一个其他元素是 $f(x)$ 的一个倍元. 我们称这个多项式 f 为 α 在 F 上的既约多项式.

重要的是要注意这个既约多项式 f 既依赖于 F 也依赖于 α，因为一个多项式的既约性依赖于域. 例如，设 $F=\mathbb{Q}[i]$，并设 α 为复数 $\sqrt{i}=\frac{1}{2}\sqrt{2}(1+i)$. α 在 $\mathbb{Q}$ 上的既约多项式为 x^4+1，但这个多项式在域 F 上分解：$x^4+1=(x^2+i)(x^2-i)$. 在 F 上 α 的既约多项式是 x^2-i. 当有几个域的时候，必须仔细搞清楚所说的是哪个域. 说一个多项式既约是模糊的. 最好说 f 在 F 上既约，或它是 $F[x]$ 的既约元.

由一个元素 $\alpha \in K$ 生成的 F 的扩域记为 $F(\alpha)$：

【2.3】 *$F(\alpha)$ 是包含 F 和 α 的最小的域.*

更一般地，如果 $\alpha_1, \cdots, \alpha_n$ 是 F 的一个扩域 K 中的元素，则记号 $F(\alpha_1, \cdots, \alpha_n)$ 将表示 K 中包含这些元素的最小的子域.

如在第十章里一样，我们把由 α 在 F 上生成的环记作 $F[\alpha]$. 它由 K 中所有可以写成系数属于 F 的 α 的多项式的元素组成：

【2.4】
$$a_n\alpha^n + \cdots + a_1\alpha + a_0, \quad a_i \in F.$$

域 $F(\alpha)$ 与 $F[\alpha]$ 的分式域同构. 其元素是形如(2.4)的元素的比[见第十章(6.7)].

【2.5】命题　*如果 α 在 F 上是超越的，则映射 $F[x] \longrightarrow F[\alpha]$ 是一个同构，因此 $F(\alpha)$ 同构于有*

理函数域 $F(x)$.

这个简单的事实有下面的结果：对于所有的超越元 α，扩域 $F(\alpha)$ 是同构的，因为它们都与有理函数域 $F(x)$ 同构. 例如，π 和 e 都是 $\mathbb{Q}$ 上的超越元（虽然我们并没有证明它们是超越元）. 因而 $\mathbb{Q}(\pi)$ 和 $\mathbb{Q}(e)$ 是同构的域，同构将 π 映到 e. 初看上去这是相当令人惊讶的. 把这些域视为实数域的子域时，同构不是连续的.

494

如果 α 是代数元，则情况大不一样：

【2.6】命题

(a) 假设 α 是 F 上的代数元，并设 $f(x)$ 是它在 F 上的既约多项式. 映射 $F[x]/(f)\longrightarrow F[\alpha]$ 是一个同构，并且 $F[\alpha]$ 是一个域. 这样，$F[\alpha]=F(\alpha)$.

(b) 更一般地，设 $\alpha_1,\cdots,\alpha_n$ 是 F 的一个扩域 K 中的代数元. 则 $F[\alpha_1,\cdots,\alpha_n]=F(\alpha_1,\cdots,\alpha_n)$.

证明　设 φ 为映射(2.2)，且 $K=F[\alpha]$. 由于 $f(x)$ 生成 $\ker\varphi$，我们知道 $F[x]/(f)$ 同构于 φ 的象[第十章(3.1)]，也就是 $F[\alpha]$. 由于 f 既约，它生成极大理想[第十一章(1.6)]. 这证明了 $F[\alpha]$ 是域. 由于 $F(\alpha)$ 与 $F[\alpha]$ 的分式域同构，它等于 $F[\alpha]$. 我们将第二部分的证明留作练习. ■

【2.7】命题　设 α 为 F 上的代数元，并设 $f(x)$ 是其既约多项式. 假设 $f(x)$ 的次数为 n，则 $(1,\alpha,\cdots,\alpha^{n-1})$ 是 $F[\alpha]$ 作为 F 上向量空间的基.

证明　这个命题是第十章中(5.7)的一种特殊情形. ■

要说清楚两个代数元 α,β 是否生成同构的域可能不太容易，虽然可用命题(2.7)给出一个必要条件：它们在 F 上的既约多项式要有相同的次数，因为这个次数是扩域作为 F-向量空间的维数. 这显然不是一个充分条件. 例如，第十一章学习的所有虚二次域都是由添加既约多项式为 2 次多项式 x^2-d 的元素 δ 得到的，但它们不都是同构的. 另一方面，如果 α 是 x^3-x+1 的根，则 $\beta=\alpha^2$ 是 x^3-2x^2+x-1 的根. 两个域 $\mathbb{Q}[\alpha]$ 和 $\mathbb{Q}[\beta]$ 实际上是相等的，尽管如果只是给出两个多项式，我们要花点时间才能看出它们是如何联系的.

容易描述这样的情形：存在一个使 F 不变而将 α 映到 β 的同构

【2.8】
$$F(\alpha)\xrightarrow{\sim}F(\beta).$$

下面的命题对于我们理解扩域是基本的：

【2.9】命题　设 $\alpha\in K$ 和 $\beta\in L$ 是 F 的两个扩域中的代数元. 存在域的同构

495

$$\sigma:F(\alpha)\xrightarrow{\sim}F(\beta),$$

它在子域 F 上是恒等映射且使 $\alpha\rightsquigarrow\beta$ 当且仅当 α 和 β 在 F 上的既约多项式是相同的.

证明　假定 $f(x)$ 是 α 和 β 在 F 上的既约多项式. 应用命题(2.6)，得到两个同构

$$F[x]/(f)\xrightarrow{\varphi}F[\alpha]\quad 和\quad F[x]/(f)\xrightarrow{\psi}F[\beta].$$

合成映射 $\sigma=\psi\varphi^{-1}$ 是所需的同构. 反之，如果存在将 α 映到 β 且在 F 上是恒等映射的同构 σ，且如果 $f(x)\in F[x]$ 是使得 $f(\alpha)=0$ 的多项式，则也有 $f(\beta)=0$[见命题(2.11)]. 因此两个元素有同一个既约多项式. ■

【2.10】定义　设 K 和 K' 是同一个域 F 的两个扩域. 一个在子域 F 上的限制为恒等映射的同构 $\varphi:K\longrightarrow K'$ 称为扩域的同构或 F-同构. 域 F 的两个扩域 K，K' 称为同构的扩域，如果存在一个 F-同构 $\varphi:K\longrightarrow K'$.

【2.11】命题 设 $\varphi: K \longrightarrow K'$ 是 F 的扩域的一个同构，并设 $f(x)$ 是系数属于 F 的多项式. 设 α 是 f 在 K 中的一个根，并设 $\alpha'=\varphi(\alpha)$ 是它在 K' 中的象. 则 α' 亦是 f 的根.

证明 设 $f(x)=a_nx^n+\cdots+a_1x+a_0$. 则 $\varphi(a_i)=a_i$ 且 $\varphi(\alpha)=\alpha'$. 由于 φ 是同态，可以如下展开：

$$\begin{aligned}0=\varphi(0)=\varphi(f(\alpha))&=\varphi(a_n\alpha^n+\cdots+a_1\alpha+a_0)\\&=\varphi(a_n)\varphi(\alpha)^n+\cdots+\varphi(a_1)\varphi(\alpha)+\varphi(a_0)\\&=a_n\alpha'^n+\cdots+a_1\alpha'+a_0.\end{aligned}$$

这证明了 α' 是 f 的根. ■

例如，多项式 x^3-2 是 $\mathbb{Q}$ 上的既约多项式. 设 α 为 2 的实立方根，并设 $\zeta=e^{2\pi i/3}$ 为 1 的一个复立方根. 则 x^3-2 的三个复根为 α，$\zeta\alpha$ 和 $\zeta^2\alpha$. 因而存在一个同构

【2.12】 $$\mathbb{Q}(\alpha)\xrightarrow{\sim}\mathbb{Q}(\zeta\alpha)$$

将 α 映到 $\zeta\alpha$. 在这种情形下 $\mathbb{Q}(\alpha)$ 的元素都是实数，但 $\mathbb{Q}(\zeta\alpha)$ 不是 $\mathbb{R}$ 的子域. 要理解同构 (2.12)，就不能再将这些域视为 $\mathbb{C}$ 的子域，而只考虑它们内部的代数结构.

第三节 扩域的次数

496

域 F 的一个扩域 K 总是可以视为一个 F-向量空间. 加法是 K 中的加法法则，K 中元素 α 用 F 的元素 c 的标量乘法定义为由这两个元素在 K 中相乘构成的积 $c\alpha$. K 作为 F-向量空间的维数称为扩域 $F\subset K$ 的*次数*. 次数是扩域的一个最简单的不变量，它虽然简单，但也是重要的. 把它记为

【3.1】 $$[K:F]=K\text{ 作为 }F\text{-向量空间的维数}.$$

例如，$\mathbb{C}$ 有 $\mathbb{R}$-基$(1, i)$，因而$[\mathbb{C}:\mathbb{R}]=2$.

如果次数$[K:F]$是有限的，则扩域 $F\subset K$ 称为一个*有限扩域*. 次数为 2 的扩域称为*二次扩域*，次数为 3 的扩域称为*三次扩域*，等等. 扩域 $F\subset K$ 的次数为 1 当且仅当 $F=K$.

术语次数来自于 $K=F(\alpha)$ 由一个代数元 α 生成的情形下. 在这一情形下，K 有基$(1, \alpha, \cdots, \alpha^{n-1})$，其中 n 是 α 的既约多项式在 F 上的次数[命题(2.7)]. 这样我们看到次数的第一个重要性质：

【3.2】命题 如果 α 在 F 上是代数元，则$[F(\alpha):F]$为 α 在 F 上既约多项式的次数.

次数也称为 α 在 F 上的*次数*. 注意一个元素 α 在 F 上次数为 1 当且仅当它是 F 中的一个元素，且 α 的次数为 ∞ 当且仅当它在 F 上是超越的.

很容易描述二次扩域.

【3.3】命题 假设域 F 的特征不为 2，即在 F 中 $1+1\neq 0$. 则任意二次扩域 $F\subset K$ 可由添加一个平方根得到：$K=F(\delta)$，其中 $\delta^2=D$ 是 F 中的一个元素. 反之，如果 δ 是 F 的扩域的元素，且如果 $\delta^2\in F$ 但 $\delta\notin F$，则 $F(\delta)$ 是一个二次扩域.

证明 我们先证明每个二次扩域由添加一个二次多项式 $f(x)\in F[x]$ 的根得到. 为此，选择 K 中不属于 F 的元素 α. 则$(1, \alpha)$是 F 上的线性无关的集合. 由于 K 作为 F 上的向量空间的维数为 2，因此$(1, \alpha)$是 K 在 F 上的基，且 $K=F[\alpha]$. 由此得到 α^2 是$(1, \alpha)$的线性组合，

设$\alpha^2=-b\alpha-c$，其中b，$c\in F$．则α是$f(x)=x^2+bx+c$的根．

由于在F中$2\neq 0$，我们可用二次公式$\alpha=\frac{1}{2}(-b+\sqrt{b^2-4c})$来解方程$x^2+b\alpha+c=0$．这可通过直接计算证明．对平方根有两种选择，其中之一给出我们选定的根α．用δ表示这个选择：$\delta=\sqrt{b^2-4c}=2\alpha+b$．则$\delta$属于$K$，且它在$F$上生成$K$．其平方是判别式$b^2-4c$，属于$F$．

命题的最后断言是显然成立的． ■

次数的第二个重要性质是在域塔中它是乘法的．

497 **【3.4】定理** 设$F\subset K\subset L$是域．则$[L:F]=[L:K][K:F]$．

证明 设$\boldsymbol{B}=(y_1,\cdots,y_n)$是$L$作为$K$-向量空间的基，并设$\boldsymbol{C}=(x_1,\cdots,x_m)$是$K$作为$F$-向量空间的基．因而$[L:K]=n$而$[K:F]=m$．我们将证明$mn$个积$\boldsymbol{P}=(\cdots,x_iy_j,\cdots)$的集合是$L$作为$F$-向量空间的基，而这将证明命题．同样的推理当$\boldsymbol{B}$或$\boldsymbol{C}$为无限时也是可行的．

设α是L的元素．由于$\boldsymbol{B}$是L在K上的基，我们可以用唯一方式记$\alpha=\beta_1y_1+\cdots+\beta_ny_n$，其中$\beta_j\in K$．由于$\boldsymbol{C}$是$K$在$F$上的基，每一$\beta_j$可以唯一表示为$\beta_j=a_{1j}x_1+\cdots+a_{mj}x_m$，而$a_{ij}\in F$．这样$\alpha=\sum_{i,j}a_{ij}x_iy_j$．这表明$\boldsymbol{P}$作为$F$-向量空间张成$L$．我们知道$\beta_j$由$\alpha$唯一确定，且由于$\boldsymbol{C}$是$K$在$F$上的基，元素$a_{ij}$由$\beta_j$唯一确定．因而它们由$\alpha$唯一确定．这表明$\boldsymbol{P}$线性无关，因而它是$L$在$F$上的基． ■

扩域塔的一个重要情形是K是给定的F的扩域并且α是K的一个元素．则由α生成的域$F(\alpha)$是一个中间域：

【3.5】 $$F\subset F(\alpha)\subset K.$$

【3.6】推论 *设K是F的一个具有有限次数n的扩域．设α是K的一个元素．则α在F上是代数的，且其次数整除n．*

为看到这一点，我们将定理(3.4)用到域$F\subset F(\alpha)\subset K$上并利用下面的事实：如果$\alpha$是代数的，则$\alpha$在$F$上的次数是$[F(\alpha):F]$，而如果$\alpha$是超越的，则$[F(\alpha):F]=\infty$．

下面是一些应用范例：

【3.7】推论 *设K是F上的素数p次的扩域，并设α是K中不属于F的元素．则α在F上的次数为p且$K=F(\alpha)$．*

因为$p=[K:F]=[K:F(\alpha)][F(\alpha):F]$．右边有一项是1．由于$\alpha\notin F$，为1的这一项不是第二项，因而$[K:F(\alpha)]=1$且$[F(\alpha):F]=p$．因此$K=F(\alpha)$．

【3.8】推论 *$\mathbb{R}[x]$的既约多项式的次数为1或2．*

在第十一章第一节已证明了这一点，但我们再次导出它：设g是既约实多项式．则g在$\mathbb{C}$中有一个根α．由于$[\mathbb{C}:\mathbb{R}]=2$，由(3.6)，$\alpha$在$\mathbb{R}$上的次数整除2．因而$g$的次数为1或2．

【3.9】例

(a) 设$\alpha=\sqrt[3]{2}$，$\beta=\sqrt[4]{5}$．考虑由在$\mathbb{Q}$上添加α和β得到的域$L=\mathbb{Q}(\alpha,\beta)$．则$[L:\mathbb{Q}]=12$．$L$包含子域$\mathbb{Q}(\alpha)$，因为$\alpha$在$\mathbb{Q}$上的既约多项式为$x^3-2$，所以它在$\mathbb{Q}$上的次数为3．因而3整除$[L:\mathbb{Q}]$．类似地，$L$包含子域$\mathbb{Q}(\beta)$而$\beta$在$\mathbb{Q}$上的次数为4，因而4整除$[L:\mathbb{Q}]$．另一方面，498 因为$\beta$是$x^4-5$的根，且这个多项式的系数属于$\mathbb{Q}(\alpha)$，故$\beta$在域$\mathbb{Q}(\alpha)$上的次数最多为4．域

链$L=\mathbb{Q}(\alpha,\beta)\supset\mathbb{Q}(\alpha)\supset\mathbb{Q}$表明$[L:\mathbb{Q}]$最多是12．因而$[L:\mathbb{Q}]=12$.

(b) 由模2约化得到多项式$f(x)=x^4+2x^3+6x^2+x+9$在$\mathbb{Q}$上既约[第十一章(4.3)]．设γ是$f(x)$的一个根．则无法用γ的有理表达式表出$\alpha=\sqrt[3]{2}$，即$\alpha\notin\mathbb{Q}(\gamma)$．由于$[\mathbb{Q}(\alpha):\mathbb{Q}]=3$，$[\mathbb{Q}(\gamma):\mathbb{Q}]=4$而3不整除4．因而不可能有$\mathbb{Q}(\gamma)>\mathbb{Q}(\alpha)$．另一方面，由于$i$在$\mathbb{Q}$上次数为2，不容易确定$i$是否属于$\mathbb{Q}(\gamma)$．(事实上，它是不属于$\mathbb{Q}(\gamma)$的.)

下面两个定理陈述了次数的乘法性质的最重要的抽象结论.

【3.10】定理 设K是F的一个扩域．则K中在F上的代数的元素构成K的一个子域.

证明 设α，β是K的代数元．要证$\alpha+\beta$，$\alpha\beta$，$-\alpha$和α^{-1}(如果$\alpha\neq 0$)也是代数的．我们注意由于α是代数的，因此$[F(\alpha):F]<\infty$．而且β在F上是代数的，因此它在更大的域$F(\alpha)$上也是代数的．因而由β在$F(\alpha)$上生成的域$F(\alpha,\beta)$是$F(\alpha)$上的有限扩张，即$[F(\alpha,\beta):F(\alpha)]<\infty$.由定理(3.4)，$[F(\alpha,\beta):F]$也有限．因而$F(\alpha,\beta)$的每个元素在$F$上是代数的(3.6)．元素$\alpha+\beta$，$\alpha\beta$等都属于$F(\alpha,\beta)$，因而它们是代数的．这证明了代数元构成一个域. ■

例如，假定$\alpha=\sqrt{a}$，$\beta=\sqrt{b}$，其中a，$b\in F$．我们确定以$\gamma=\alpha+\beta$为根的多项式．为此计算γ的幂，并且在可能时用关系$\alpha^2=a$，$\beta^2=b$简化结果．然后找出这些幂之间的线性关系：

$$\gamma^2=\alpha^2+2\alpha\beta+\beta^2=(a+b)+2\alpha\beta$$

$$\gamma^4=(a+b)^2+4(a+b)\alpha\beta+4\alpha^2\beta^2=(a^2+6ab+b^2)+4(a+b)\alpha\beta.$$

我们不需要其他的幂，因为可以由这两个等式消去$\alpha\beta$而得到$\gamma^4-2(a+b)\gamma^2+(a-b)^2=0$．这样$\gamma$是系数属于$F$的多项式

$$g(x)=x^4-2(a+b)x^2+(a-b)^2$$

的根，这正是所需要的.

如果给出α和β的既约多项式，待定系数法总会给出一个使得像$\alpha+\beta$这样的元素为其根的多项式．假设两个元素α，β的次数为d_1，d_2，并设$n=d_1d_2$．$F(\alpha,\beta)$的每个元素都是n个单项式$\alpha^i\beta^j$($0\leqslant i<d_1$，$0\leqslant j<d_2$)的一个系数属于F的线性组合．这是因为$F(\alpha,\beta)=F[\alpha,\beta]$(2.6)，而这些单项式张成了$F[\alpha,\beta]$．给定一个元素$\gamma\in F(\alpha,\beta)$，我们将幂1，$\gamma$，$\gamma^2$，…，$\gamma^n$写为这些单项式的一个系数属于$F$的线性组合．由于有$n+1$个幂$\gamma^\nu$，而只有$n$个单项式$\alpha^i\beta^j$，因此这些幂线性相关．一个线性相关的关系确定一个以γ为根的系数属于F的多项式.

499

但有一点使问题变得复杂．设$g(x)$是我们以这种方式找到的以γ为根的多项式．这个多项式可能是可约的．例如，虽然α，β不属于F，但可能碰巧γ实际上属于域F．如果这样，我们描述的方法不可能产生其既约多项式$x-\gamma$．确定γ在F上的既约多项式比较困难.

F的扩域K称为代数扩域，或称K在F上是代数的，如果它的所有元素都是代数的.

【3.11】定理 设$F\subset K\subset L$是域．如果L在K上是代数的且K在F上是代数的，则L在F上是代数的.

证明 我们要证明每一个元素$\alpha\in L$在F上是代数的．已知α在K上是代数的，因而某个形如

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

的等式成立，其中 a_0，…，$a_{n-1}\in K$. 因而 α 在由 a_0，…，a_{n-1} 在 F 上生成的域 $F(a_0,\cdots,a_{n-1})$ 上是代数的. 注意每个系数 a_i 属于 K，因而在 F 上是代数的. 考虑通过逐个添加元素 a_0，…，a_{n-1}，α 得到的域链

$$F\subset F(a_0)\subset F(a_0,a_1)\subset\cdots\subset F(a_0,a_1,\cdots,a_{n-1})\subset F(a_0,a_1,\cdots,a_{n-1},\alpha).$$

对每个 i，a_{i+1} 在 $F(a_0,\cdots,a_i)$ 上是代数的，因为它在 F 上是代数的. 还有，α 在 $F(a_0,a_1,\cdots,a_{n-1})$ 上是代数的. 因而链中的每个扩域都是有限的. 由定理(3.4)，$F(a_0,a_1,\cdots,a_{n-1},\alpha)$ 在 F 上的次数有限. 因而由推论(3.6)，α 在 F 上是代数的. ■

第四节　直尺圆规作图

有一个著名的定理断言：诸如三等分一个角之类的某些几何构造不能只用直尺和圆规作出. 我们现在用扩域次数的概念证明其中一些断言.

下面是直尺和圆规作图的基本规则：

【4.1】(a) 给定平面上的两个点作为开始. 这两个点被认为是作出的.

(b) 如果作了两个点，可过它们作一条直线，或者作一个以其中一个为圆心并过另一点的圆. 这样的直线和圆被认为是作出的.

500

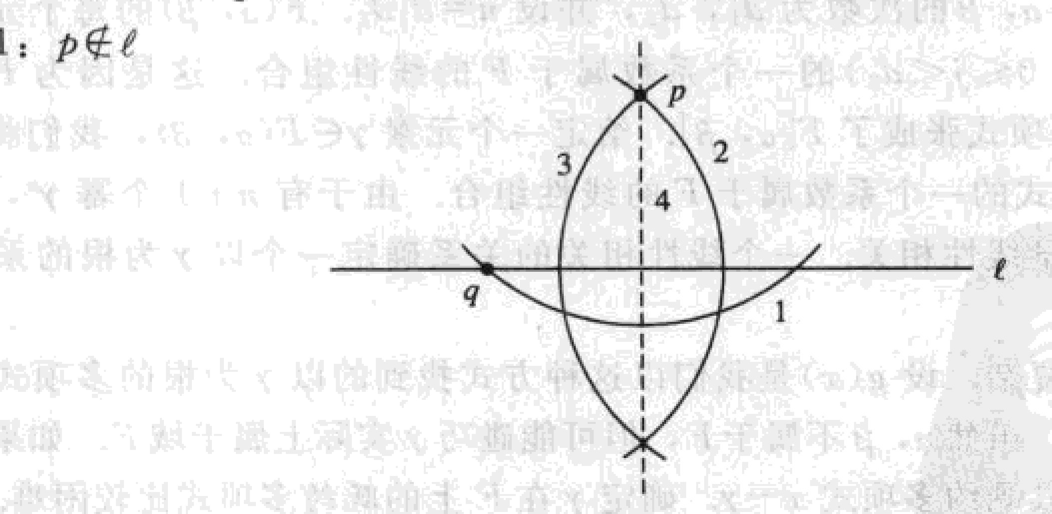
(c) 已作出的直线和圆的交点被认为是作出的.

注意我们的直尺只能用于过作出的点作直线. 不能用它来度量长度. 有时将其称为"直边"来明确这一点.

我们将从一些熟知的作图开始来描述所有可能的作图. 在每个图中，直线和圆按标出的顺序作出.

【4.2】作图　过一个点 p 作一条与直线 ℓ 垂直的直线.

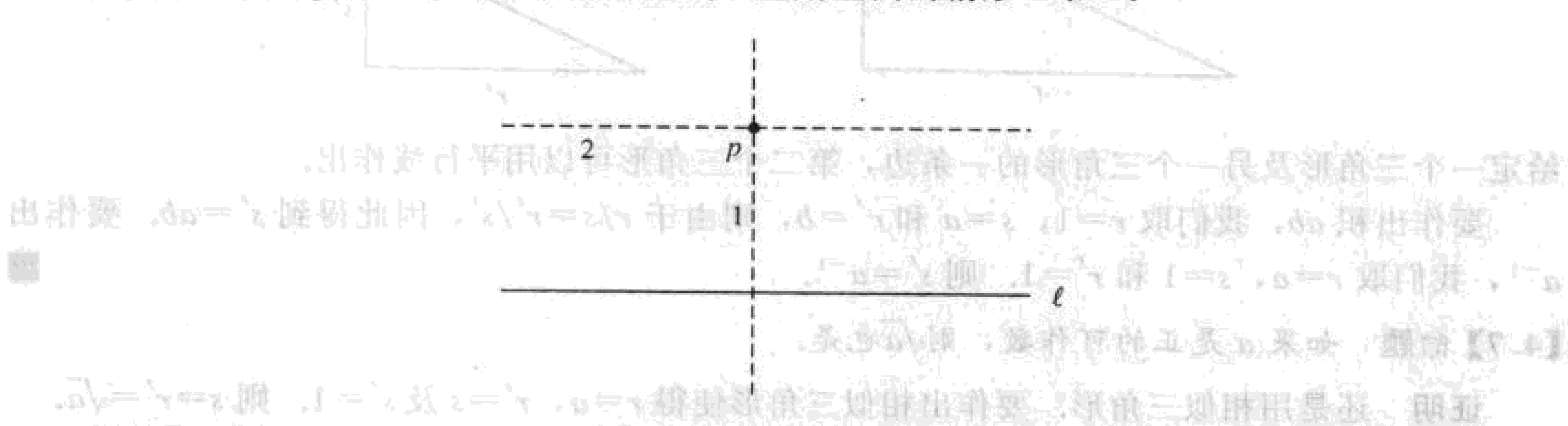
情形 1：$p\notin\ell$



这个作图对任意不在垂线上的点 $q\in\ell$ 都可行. 然而最好不要任意地选点，因为如果任意选点，那么将难以追踪哪些点是我们作出的而哪些点只不过是我们任意选出的. 每当需要任意点时，我们将作一个特别的点来用.

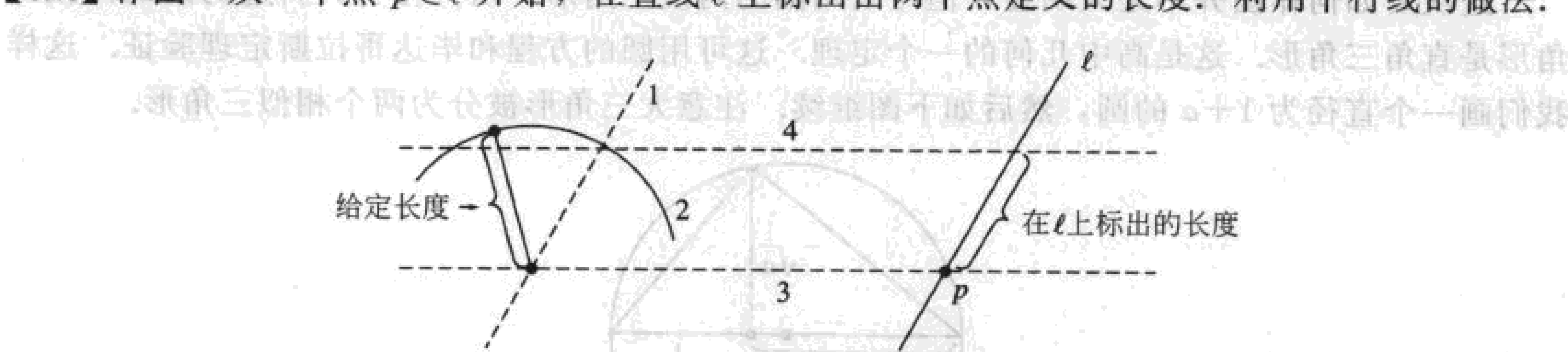
情形 2：$p\in\ell$

【4.3】作图　过点 p 作一条与 ℓ 平行的直线．应用上面的情形 1 和 2：

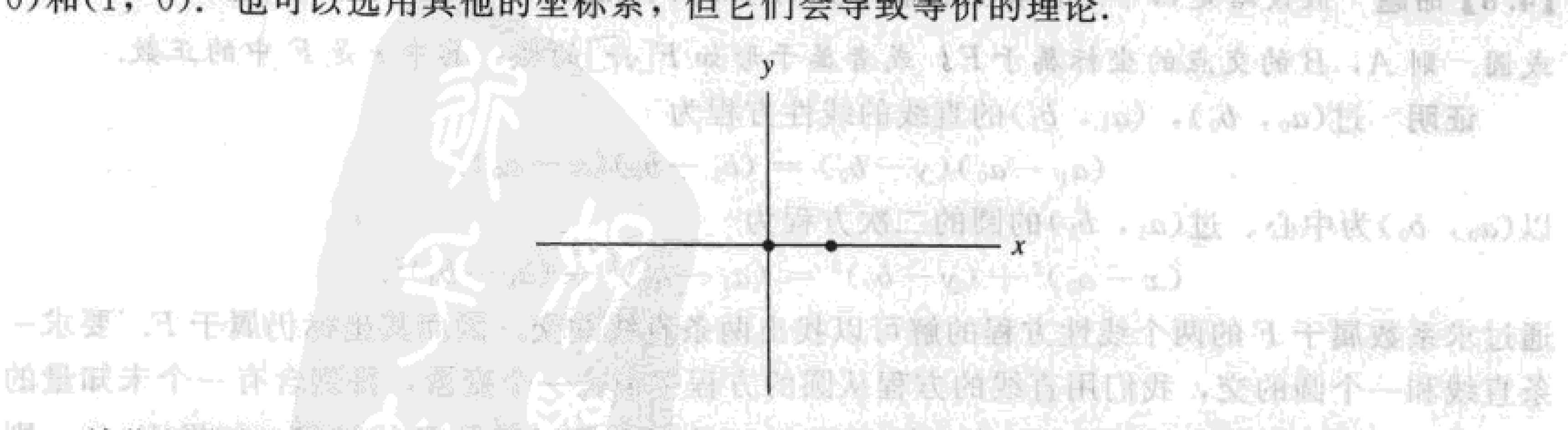


501

【4.4】作图　从一个点 $p\in\ell$ 开始，在直线 ℓ 上标出由两个点定义的长度．利用平行线的做法．



这些作图使我们能在平面上引入笛卡儿坐标系而使得在开始时给定的两个点的坐标为(0，0)和(1，0)．也可以选用其他的坐标系，但它们会导致等价的理论．



单位长度是最先给定的两点间的距离，一个实数 a 称为可作的，如果其绝对值 $|a|$ 是两个可作点间的距离．

502 **【4.5】命题** 点 $p=(a, b)$是可作的当且仅当其笛卡儿坐标 a 和 b 都是可作的数.

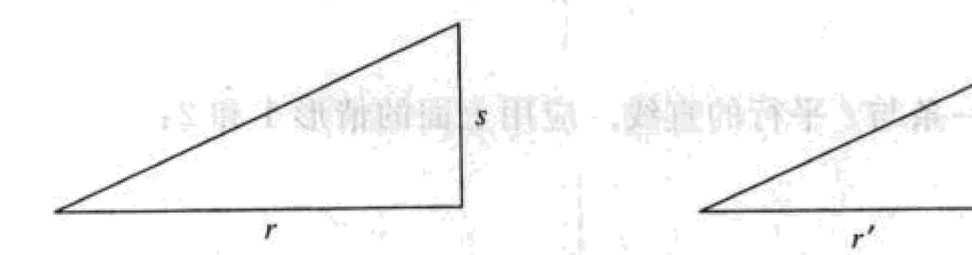
证明 这由上述作图得到. 给定点 p，可以通过作到坐标轴的垂线作出其坐标. 反之，如果 a，b 是给定的可作数，则可用(4.4)在两个轴上标出 a，b 并作垂线而作出点 p. ■

【4.6】命题 可作数构成$\mathbb{R}$ 的子域.

证明 我们将证明如果 a，b 是正可作数，则 $a+b$，ab，$a-b$(如果 $a>b$)和 a^{-1}(如果 $a\neq 0$)也是可作的. a，b 为负数的情形容易得到.

加法和减法通过用(4.4)在直线上标出长度作出.

对乘法，我们用相似直角三角形：



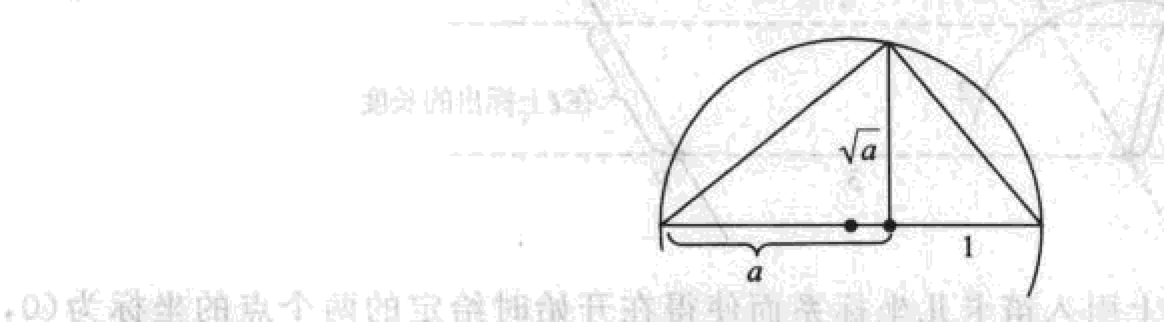
给定一个三角形及另一个三角形的一条边，第二个三角形可以用平行线作出.

要作出积 ab，我们取 $r=1$，$s=a$ 和 $r'=b$，则由于 $r/s=r'/s'$，因此得到 $s'=ab$. 要作出 a^{-1}，我们取 $r=a$，$s=1$ 和 $r'=1$. 则 $s'=a^{-1}$. ■

【4.7】命题 如果 a 是正的可作数，则$\sqrt{a}$也是.

证明 还是用相似三角形. 要作出相似三角形使得 $r=a$，$r'=s$ 及 $s'=1$. 则 $s=r'=\sqrt{a}$.

这次要如何作图并不是太明显，但可以用圆的内接三角形. 以直径为其斜边的圆的内接三角形是直角三角形. 这是高中几何的一个定理. 这可用圆的方程和毕达哥拉斯定理验证. 这样我们画一个直径为 $1+a$ 的圆，然后如下图继续. 注意大三角形被分为两个相似三角形.



【4.8】命题 假设给定四个点，其坐标属于$\mathbb{R}$ 的子域 F. 设 A，B 是用这些给定点作出的直线或圆. 则 A，B 的交点的坐标属于 F，或者属于形如 $F[\sqrt{r}]$的域，其中 r 是 F 中的正数. 503

证明 过(a_0, b_0)，(a_1, b_1)的直线的线性方程为

$$(a_1-a_0)(y-b_0)=(b_1-b_0)(x-a_0).$$

以(a_0, b_0)为中心、过(a_1, b_1)的圆的二次方程为

$$(x-a_0)^2+(y-b_0)^2=(a_1-a_0)^2+(b_1-b_0)^2.$$

通过求系数属于 F 的两个线性方程的解可以找出两条直线的交. 因而其坐标仍属于 F. 要求一条直线和一个圆的交，我们用直线的方程从圆的方程中消去一个变量，得到含有一个未知量的二次方程. 这个方程在域 $F(\sqrt{D})$中有解，其中 D 是判别式，它是 F 的元素. 如果 $D<0$，则直线和圆不相交.

考虑两个圆的交，比如

$$(x-a_1)^2+(y-b_1)^2=r_1{}^2 \quad \text{和} \quad (x-a_2)^2+(y-b_2)^2=r_2{}^2,$$

其中 a_i，b_i，$r_i \in F$. 一般来说，求一对二元二次方程的解需要解四次方程. 我们在这里很幸运：两个二次方程的差是线性方程，可以像前面一样，用它来消去一个变量. ■

【4.9】定理 设 a_1，…，a_m 是可作实数. 存在一个子域链 $\mathbb{Q}=F_0\subset F_1\subset F_2\subset\cdots\subset F_n=K$ 使得

(i) K 是 $\mathbb{R}$ 的子域；

(ii) a_1，…，$a_m\in K$；

(iii) 对每个 $i=0$，…，$n-1$，域 F_{i+1} 由在 F_i 上添加一个不是 F_i 中数的平方的正数 $r_i\in F_i$ 的平方根得到.

反之，设 $\mathbb{Q}=F_0\subset F_1\subset F_2\subset\cdots\subset F_n=K$ 是 $\mathbb{R}$ 的一个满足(iii)的子域链. 则 K 的每个元素是可作的.

证明 引入坐标系使得原来给定的点的坐标属于 $\mathbb{Q}$. 作一个数 a_i 涉及画直线和圆以及取它们的交. 因而第一个断言由命题(4.8)通过数学归纳法得到. 反之，如果给定这样一个域塔，则由命题(4.6)和(4.7)，其元素是可作的.

【4.10】推论 如果 a 是一个可作的实数，则它是代数的且它在 $\mathbb{Q}$ 上的次数是 2 的幂.

因为在(4.9)的域链中，F_{i+1} 在 F_i 上的次数为 2，因此 $[K:\mathbb{Q}]=2^n$. 推论(3.6)告诉我们 a 的次数整除 2^n，因此是 2 的一个幂.

504

推论(4.10)的逆不成立. 存在 $\mathbb{Q}$ 上次数为 4 的实数 a，但它不是可作的. 后面将用伽罗瓦理论证明这一点.

我们现在可以证明某些几何作图的不可能性. 办法是证明如果某个作图是可能的，则也将可能作出一个在 $\mathbb{Q}$ 上次数不是 2 的幂的代数数. 这与(4.10)矛盾.

作为第一个例子我们讨论三等分角. 必须仔细地提出问题，因为许多角是可以三等分的，例如 45°角. 叙述这一问题通常的方式是：求一个对任意给定的角都可行的作图法.

为了尽可能地加以明确，我们说一个角 θ 是可作的是指其余弦 $\cos\theta$ 是可作的. 其他等价的定义也是可能的. 例如，在这个定义下，θ 是可作的当且仅当过原点且与 x-轴夹角为 θ 的直线是可作的. 或者说 θ 是可作的当且仅当能够作出任意两条夹角为 θ 的直线.

现在给出了角 θ(比如标出其在 x-轴上的余弦)，它们提供了在假定的三等分角中可以使用的新的信息. 为分析这个新信息带来的后果，我们应该从头开始，并在一开始除了两点之外，还有一个给定的长度($=\cos\theta$)，这时确定所有可作的图. 我们给出一个特别的角 θ，它具有下面的性质：

【4.11】 (i) θ 是可作的，并且(ii) $\frac{1}{3}\theta$ 是不可作的.

第一个条件告诉我们作为给出的角度 θ，它并没有提供新的信息：如果当角 θ 给出时可被三等分，不给出时它也能被三等分. 第二个条件告诉我们没有三等分角的一般方法，因为没有三等分角 θ 的方法.

$\theta=60°$就是这样的角. 因为 $\cos60°=\frac{1}{2}$，所以一个 60°角是可作的. 另一方面，不可能作

出 20°角. 为说明这一点，我们将证明 cos20°是$\mathbb{Q}$上 3 次代数数. 于是推论(4.10)表明 cos20°不是可作的，因而 60°角不能被三等分.

可用正弦和余弦的加法公式来证明等式

【4.12】
$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

取 $\theta=20°$ 及 $\alpha=\cos 20°$，我们得到 $\frac{1}{2}=4\alpha^3-3\alpha$，或 $8\alpha^3-6\alpha-1=0$.

【4.13】引理　*多项式 $f(x)=8x^3-6x-1$ 在$\mathbb{Q}$上既约.*

证明　只需要对线性因子 $ax+b$ 进行验证，其中 a，b 是整数，并且 a 整除 8 而 $b=\pm 1$. 另一个证明既约性的办法是验证 f 没有模 5 的根. ■

505

这个引理告诉我们 α 在$\mathbb{Q}$上次数为 3，因此它不能被作出.

作为另一个例子，我们证明正 7-边形是不可作的. 这与上面的问题类似：作 20°角等价于作正 18 边形. 用 θ 表示角 $2\pi/7$ 并设 $\zeta=\cos\theta+i\sin\theta$，则 ζ 是多项式 $x^6+x^5+\cdots+1=0$ 的一个根，而这个多项式是既约的[第十一章(4.6)]. 因此 ζ 在$\mathbb{Q}$上次数为 6. 如果正 7-边形是可作的，则 $\cos\theta$ 和 $\sin\theta$ 都是可作的数，因此由定理(4.9)，它们将属于$\mathbb{Q}$上次数为 2^n 的实扩域. 将这个域称作 K 并考虑扩域 $K[i]$. 这个扩域的次数为 2. 因而$[K[i]:\mathbb{Q}]=2^{n+1}$. 但 $\zeta=\cos\theta+i\sin\theta\in K[i]$. 这与 ζ 的次数为 6 矛盾(3.6).

注意到这一论证不仅特别针对数 7. 它可以用于任意的素整数 p，只要既约多项式 $x^{p-1}+\cdots+x+1$的次数 $p-1$ 不是 2 的幂就行了.

【4.14】推论　*设 p 是素整数. 如果正 p-边形可用尺规作出，则对某个整数 r，有 $p=2^r+1$.*

高斯证明了其逆：如果一个素数有 2^r+1 的形式，则正 p-边形是可作的. 例如正 17-边形可用直尺和圆规作出. 我们将在下章学习如何证明这个结论.

第五节　根的符号添加

到目前为止，我们一直用复数的子域作为我们的例子. 创建这些域不需要抽象的构造(除了从$\mathbb{R}$到$\mathbb{C}$的构造是抽象的以外). 根据需要，可以简单地在有理数上添加复数并使用它们生成的子域. 但有限域和函数域不是类似于$\mathbb{C}$这样一个我们熟悉的、包含一切的域的子域，因而必须构造这些域. 构造它们的基本工具是在第十章第五节所学的在环上添加元素. 在这里把它应用到开始的环是一个域 F 的情形.

我们复习这一构造过程. 给定系数属于 F 的多项式 $f(x)$，可以添加一个满足多项式方程 $f(\alpha)=0$ 的元素 α 到 F. 抽象过程是构造多项式环 $F[x]$，然后取其商环

【5.1】
$$R' = F[x]/(f).$$

这个构造总是产生环 R' 及同态 $F\longrightarrow R'$，使得 x 的剩余$\bar{x}$满足关系 $f(\bar{x})=0$.

然而我们要构造的不是环，而是域，在这里域上多项式的理论起了作用. 这个理论告诉我们主理想(f)是极大理想当且仅当 f 是既约的[第十一章(1.6)]. 因而环 R'是一个域当且仅当 f 是一个既约多项式.

506

【5.2】引理　*设 F 是一个域，并设 f 是 $F(x)$ 中的既约多项式. 则环 $K=F(x)/(f)$ 是 F 的扩*

域，x 的剩余$\overline{x}$是 $f(x)$在 K 中的根.

证明 因为(f)是一个极大理想，所以环 K 是个域. 而且，因为 F 是域，所以将 F 中的元素映到常多项式的剩余的同态 $F\longrightarrow K$ 是一个单射. 因而可将 F 等同于其象，也就是 K 的一个子域. 在这一等同的意义下，域 K 成为 F 的一个扩域. 最后，$\overline{x}$满足方程 $f(\overline{x})=0$，这表明它是 f 的一个根. ■

【5.3】命题 设 F 是域，并设 $f(x)$是 $F(x)$中正次数的首一多项式. 存在 F 的扩域 K 使得 $f(x)$在 K 上分解成为线性因子的乘积.

证明 对 f 的次数用归纳法. 第一种情形是 f 在 F 中有一个根 α，则存在某个多项式 g 使得 $f(x)=(x-\alpha)g(x)$. 如果这样，则用 g 代替 f 并由归纳结束证明. 否则，选择 $f(x)$的既约因子 $g(x)$. 由引理(5.2)，存在 F 的一个扩域，称为 F_1，在其中 $g(x)$有一个根 α. 我们用 F_1 代替 F 而将其化为第一种情形. ■

正如我们所见，多项式环 $F[x]$是研究域 F 的扩域的一个重要工具. 当同时涉及两个域时，它们的多项式环之间相互关联. 这种相互关联并不会带来严重的困难，我们将需要指出的要点都集中在这里而不是分散在书中各处来加以叙述.

注意到如果 K 是 F 的扩域，则多项式环 $K[x]$包含 $F[x]$为其子环. 因而在环 $F[x]$中进行的计算在 $K[x]$中也成立.

【5.4】命题 设 f 和 g 是系数属于域 F 的多项式，并设 K 是 F 的扩域.

(a) 不论在 $F[x]$中还是在 $K[x]$中，由 f 对 g 作的带余除法得到相同的答案.

(b) f 在 $K[x]$中整除 g 当且仅当 f 在 $F[x]$中整除 g.

(c) 不论在 $F[x]$中还是在 $K[x]$中，f 和 g 的首一最大公因式 d 都是同一个.

(d) 如果 f 和 g 在 K 中有公共根，则它们在 $F[x]$中不是互素的. 反之，如果 f 和 g 在 $F[x]$中不是互素的，则存在一个扩域 L，它们在其中有公共根.

(e) 如果 f 在 $F[x]$中是既约的且 f 和 g 在 $K[x]$中有公共根，则 f 在 $F[x]$中整除 g.

证明 (a) 在 $F[x]$中作除法：$g=fq+r$. 这个等式在更大的环 $K[x]$中也成立，因为 r 的次数低于 f，或者为 0，所以用 f 继续作带余除法是不可能的.

507

(b) 这是(a)中余式为零的情形.

(c) 设 d，d'表示 f 和 g 在 $F[x]$中和在 $K[x]$中的首一最大公因式. 则 d 也是在 $K[x]$中的一个公因式. 因而由 d'的定义，在 $K[x]$中 d 整除 d'. 除此之外，我们知道对于某些元素 p，$q\in F[x]$，d 具有 $d=pf+qg$ 的形式. 由于 d'整除 f 和 g，它也整除 $pf+qg=d$. 这样 d 和 d'在$K[x]$中相伴，并且由于它们是首一的，因此它们相等.

(d) 如果 α 是 f 和 g 在 K 中的公共根. 则 $x-\alpha$ 是 f 和 g 在 $K[x]$中的公因式. 因而它们在 $K[x]$中的最大公因式不为 1. 由(c)，它们在 $F[x]$中的最大公因式也不为 1. 反之，如果 f 和 g 在 $F[x]$中有一个次数>0 的公因式 d，则由(5.3)，d 在某个扩域 L 中有一个根. 这个根就是 f 和 g 的一个公共根.

(e) 如果 f 既约，则它在 $F[x]$中仅有的因式为 1，f 及其相伴元. (d)告诉我们 f 和 g 在 $F[x]$中的最大公因式不是 1. 因而它是 f. ■

本节最后一个主题涉及多项式 $f(x)$ 的导数 $f'(x)$. 在代数中导数是用微积分中求多项式函数的微分的规则计算的. 即定义 x^n 的导数为多项式 nx^{n-1}，并且如果 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$，则

【5.5】
$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1.$$
公式中的整系数通过同态 $\mathbb{Z}\longrightarrow F$ 解释为 F 中的元素[第十章(3.18)]. 因而导数是系数属于同一个域的多项式. 可以证明像微分的乘法法则那样的法则成立.

虽然微分是一个代数过程，没有什么道理臆想它会有很大的代数意义；然而它的确是有的. 对于我们，导数最重要的性质是它可以被用来识别多项式的重根.

【5.6】引理 设 F 是域，设 $f(x)\in F[x]$ 是一个多项式，并设 $\alpha\in F$ 是 f 的一个根. 则 α 是重根，也就是说 $(x-\alpha)^2$ 整除 $f(x)$ 当且仅当它同时是 $f(x)$ 和 $f'(x)$ 的根.

证明 如果 α 是 f 的一个根，则 $x-\alpha$ 整除 f：$f(x)=(x-\alpha)g(x)$. 于是 α 是 g 的根当且仅当它是 f 的一个重根. 由微分的乘法法则，
$$f'(x)=(x-\alpha)g'(x)+g(x)$$
代入 $x=\alpha$，这表明 $f'(\alpha)=0$ 当且仅当 $g(\alpha)=0$. ■

【5.7】命题 设 $f(x)\in F[x]$ 是一个多项式. 存在 F 的扩域 K 使得 f 在其中有重根当且仅当 f 与 f' 不是互素的.

508

证明 如果 f 在 K 中有一个重根，则由引理(5.6)，f 与 f' 在 K 中有公共根，因而它们在 K 中不互素. 因此它们在 F 上也不互素. 反之，如果 f 与 f' 不互素，则它们在某个扩域 K 中有公共根，因此 f 在这个域中有一个重根. ■

下面是导数在域论中最重要的应用之一：

【5.8】命题 设 f 是 $F[x]$ 中的一个既约多项式. 则除非导数 f' 是零多项式，否则 f 在 F 的任意扩域中没有重根. 特别地，如果 F 是特征为零的域，则 f 没有重根.

证明 由前面的命题，必须证明除非 f' 是零多项式，否则 f 与 f' 是互素的. 由于 f 是既约的，它与另一个多项式 g 有非常数公因子仅有的可能情形是 f 整除 g(5.4e). 而如果 f 整除 g，则 $\deg g\geq\deg f$，或者 $g=0$. 现在导数 f' 的次数小于 f 的次数. 因而除非 $f'=0$，否则 f 和 f' 没有非常数公因子，这正是所要证的. 在特征为零的域中非常数多项式的导数不等于零. ■

当 F 的特征为素数 p 时，非常数多项式 $f(x)$ 的导数可以恒等于零. 当在 f 中出现的每个单项式的指数都被 p 整除时就会发生这种情形. 在特征为 5 时导数为零的多项式的一个典型例子是
$$f(x)=x^{15}+ax^{10}+bx^5+c,$$
其中 a，b，c 是 F 中的任意元素. 由于这个多项式的导数恒等于零，因此它在任意扩域中的根都是重根. 这个多项式是否既约依赖于 F 也依赖于 a，b，c.

第六节　有　限　域

本节描述有有限多个元素的全体的域. 在第一节我们指出一个有限域 K 必含有素域 $\mathbb{F}_p$ 中的一个，且由于 K 是有限的，它作为这个域上的向量空间当然是有限维的. 我们用 F 表示 $\mathbb{F}_p$，并用 r 表示次数 $[K:F]$. 作为 F-向量空间，K 与空间 F^r 同构，而这个空间包含 p^r 个元素. 因

而一个有限域的阶总是一个素数的幂．习惯上用字母 q 表示这个数：

【6.1】
$$q = p^r = |K|.$$

当说到有限域时，p 总是表示一个素数而 q 表示 p 的幂，它是域中元素的个数，或阶．

q 个元素的域常常记为 $\mathbb{F}_q$．我们将证明所有具有同样多元素的域都是同构的，因而这个记号并不太含糊．然而，当 $r>1$ 时，同构不是唯一的．

509

除了素域 $\mathbb{F}_p$ 外，最简单的有限域是 4 阶域 $K=\mathbb{F}_4$．在 $\mathbb{F}_2[x]$ 中存在唯一的 2 次既约多项式 $f(x)$，即

【6.2】
$$f(x) = x^2 + x + 1$$

［见第十一章(4.3)］，域 K 由添加 $f(x)$ 的一个根 α 到 $F=\mathbb{F}_2$ 上得到：

$$K \approx F[x]/(x^2 + x + 1).$$

因为 α 的次数为 2，所以这个域的阶为 4，这告诉我们作为域 F 上的向量空间 K 的维数为 2．

集合$(1, \alpha)$构成 K 在 V 上的基，因而 K 的元素是这两个元素的四个线性组合，系数为 0，1(模 2)．这四个元素是

【6.3】
$$\{0,1,\alpha,1+\alpha\} = \mathbb{F}_4$$

元素 $1+\alpha$ 是多项式 $f(x)$ 在 K 中的第二个根．在 K 中计算要用到关系 $1+1=0$ 及 $\alpha^2+\alpha+1=0$．不要将域 $\mathbb{F}_4$ 与环 $\mathbb{Z}/(4)$ 混淆起来！

下面是关于有限域的主要事实：

【6.4】定理 设 p 是一个素数，并设 $q=p^r$ 是 p 的幂，其中 $r\geqslant 1$．

(a) 存在 q 阶域．

(b) 任意两个 q 阶域同构．

(c) 设 K 是一个 q 阶域．K 的非零元素的乘法群 $K^\times$ 是一个 $q-1$ 阶循环群．

(d) K 的元素是多项式 x^q-x 的根．这个多根式的根互不相同，并且它在 K 中分解为线性因式的乘积．

(e) $\mathbb{F}_q[x]$ 的每一个 r 次既约多项式是 x^q-x 的因式．x^q-x 在 $\mathbb{F}_q[x]$ 中的既约因式正好是 $\mathbb{F}_q[x]$ 中次数整除 r 的既约多项式．

(f) q 阶域 K 含有 $p'=p^k$ 阶子域当且仅当 k 整除 r．

这个定理的证明并不难，但由于它由若干部分组成，因此证明需要花点时间．我们先看一些结果以启示其证明．

(c)的惊人的地方是 K 的所有非零元素可以写为单独一个适当选择的元素的幂．即使对素域 $\mathbb{F}_p$ 这也不是明显的．例如，3 的剩余生成 $\mathbb{F}_7^\times$．其幂 3^0，3^1，3^2，…按以下顺序列出 $\mathbb{F}_7$ 的非零元素：

【6.5】
$$\mathbb{F}_7^\times = \{1,3,2,6,4,5\}.$$

510

作为另一个例子，2 是 $\mathbb{F}_{11}^\times$ 的生成元，其幂按以下顺序列出群的元素：

【6.6】
$$\mathbb{F}_{11}^\times = \{1,2,4,8,5,10,9,7,3,6\}.$$

循环群 $\mathbb{F}_p^\times$ 的生成元称为模 p 的本原元素．注意定理并没有告诉我们如何求出本原元素，

只说存在一个这样的元素. 哪个模 p 的剩余是本原元素是不清楚的，但给定一个小素数 p，可以用反复实验的方法找到一个本原元素.

现在有两个列出域$\mathbb{F}_p$的非零元素的方法，一个用加法，一个用乘法：

【6.7】 $$\mathbb{F}_p^\times=\{1,2,3,\cdots,p-1\}=\{1,v,v^2,\cdots,v^{p-2}\},$$

其中 v 是模 p 的本原元素. 根据特定的情形，对于计算来说这两个列出元素的方法中总有一个会是最好的.

当然素域的加法群$\mathbb{F}_p^+$ 总是一个 p 阶循环群. 素域的加法和乘法结构都非常简单：它们是循环的. 但由分配律所控制的$\mathbb{F}_p$的域结构将二者以一种神秘的方式组合起来.

定理中(e)也是惊人的. 它是多项式模 p 因式分解的许多方法的基础. 作为例子，看一些 q 是 2 的幂的情形：

【6.8】例

(a) 域$\mathbb{F}_4$ 的元素是多项式

【6.9】 $$x^4-x=x(x-1)(x^2+x+1)$$

的根. 在这种情形，x^4-x 在$\mathbb{Z}[x]$中的既约因子在$\mathbb{F}_2[x]$中正好也是既约的. 注意因为$\mathbb{F}_4$ 包含$\mathbb{F}_2$，所以因子 x^2-x 在这里出现.

由于是在特征 2 的情形，符号是没有关系的：$x-1=x+1$.

(b) 8 阶域$\mathbb{F}_8$ 在素域$\mathbb{F}_2$ 上次数为 3. 其元素是$\mathbb{F}_2[x]$中多项式

【6.10】 $$x^8-x=x(x-1)(x^3+x+1)(x^3+x^2+1)$$

的根. 因而$\mathbb{F}_8$ 中不属于$\mathbb{F}_2$ 的六个元素分成两类：x^3+x+1 的三个根和 x^3+x^2+1 的三个根.

(6.10)的三次因式是$\mathbb{F}_2[x]$的两个三次既约多项式[见第十一章(4.3)]. 注意这个多项式在整数环上的既约因子分解是

【6.11】 在$\mathbb{Z}[x]$ 中有 $$x^8-x=x(x-1)(x^6+x^5+\cdots+x+1).$$

第三个因子是模 2 可约的.

要在域$\mathbb{F}_8$ 中计算，可选择三次根之一，比如 x^3+x+1 的根 β. 则$(1,\beta,\beta^2)$是$\mathbb{F}_8$ 在$\mathbb{F}_2$ 上作为向量空间的一个基. $\mathbb{F}_8$ 的元素是系数为 0，1 的八个线性组合：

[511]

【6.12】 $$\mathbb{F}_8=\{0,1,\beta,1+\beta,\beta^2,1+\beta^2,\beta+\beta^2,1+\beta+\beta^2,\}.$$

在$\mathbb{F}_8$ 中的利用关系 $\beta^3+\beta+1=0$ 进行计算.

注意到$\mathbb{F}_4$ 不包含在$\mathbb{F}_8$ 之中. 因为$[\mathbb{F}_8:\mathbb{F}_2]=3$，$[\mathbb{F}_4:\mathbb{F}_2]=2$，而 2 不整除 3，因而包含关系是不可能的.

(c) 域$\mathbb{F}_{16}$：多项式 $x^{16}-x=x(x^{15}-1)$在$\mathbb{Z}[x]$中被 x^3-1 和 x^5-1 整除. 在整数上作除法给出因子分解

【6.13】 $$x^{16}-x=x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^8-x^7+x^5-x^4+x^3-x+1).$$

这是在$\mathbb{Z}[x]$中的既约因子分解. 但在$\mathbb{F}_2[x]$中，8 次因子不是既约的，并且

【6.14】 $$x^{16}-x=x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1).$$

这一分解显示了$\mathbb{F}_2[x]$的三个 4 次既约多项式. 注意 x^4-x 的因子出现在 $x^{16}-x$ 的因子之中. 这与$\mathbb{F}_{16}$包含$\mathbb{F}_4$ 这一事实是一致的.

现在将开始定理(6.4)的证明. 我们按下面的顺序对其各部分加以证明：(d), (c), (a), (b), (e)和(f).

定理(6.4d)的证明 设 K 是 q 阶域. 乘法群 $K^{\times}$ 的阶为 $q-1$. 因而任意元 $\alpha\in K^{\times}$ 的阶整除 $q-1$：$\alpha^{q-1}=1$. 这表明 α 是多项式 $x^{q-1}-1$ 的根. 剩下的 K 中的元(也就是零)是多项式 x 的根. 因而 K 的每一个元素是 $x(x^{q-1}-1)=x^q-x$ 的一个根. 因为这个多项式在 K 中有 q 个不同的根，在这个域中它分解为线性因子的乘积：

【6.15】
$$x^q-x=\prod_{\alpha\in K}(x-\alpha).$$

这证明了定理的(d). ■

定理(6.4c)的证明 域 F 中的 n 次单位根指的是 n 次幂为 1 的元素 α. 这样 α 是 n 次单位根当且仅当它是多项式

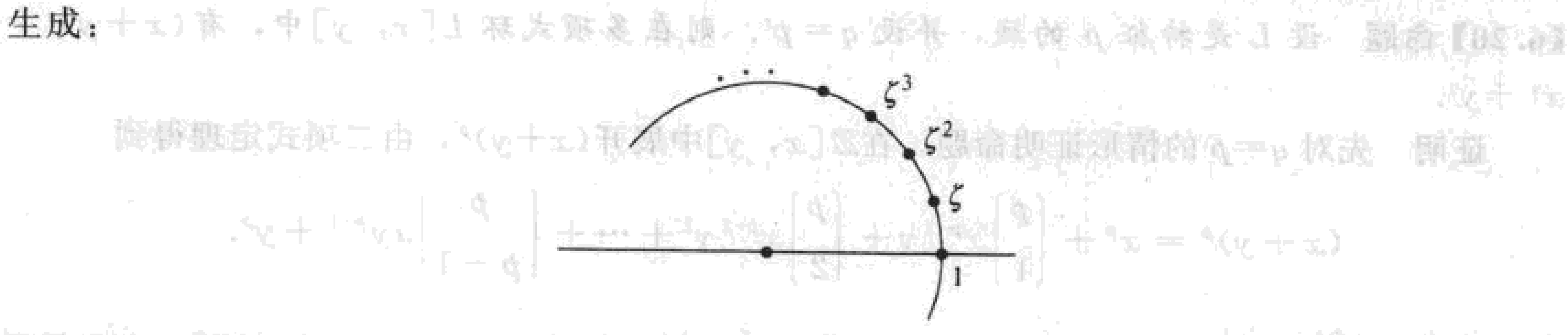
【6.16】
$$x^n-1$$

的根，或当且仅当它作为乘法群 $F^{\times}$ 的元素的阶整除 n. 有 q 个元素的有限域的非零元素是 $q-1$ 次单位根.

在复数域中，n 次单位根构成一个 n 阶循环群，由元素

【6.17】
$$\zeta_n=e^{2\pi i/n}$$

生成：



一个域中不必有许多单位根. 例如，仅有的实单位根为 ±1. 但复数的一个性质在任意域上成立：任意域中的 n 次单位根构成一个循环群. 例如，在 4 阶域 $K=\mathbb{F}_4$ 中，群 $K^{\times}$ 是由 α 生成的 3 阶循环群. [见(6.3).]

【6.18】命题 设 F 是域，并设 H 是乘法群 $F^{\times}$ 的 n 阶有限子群. 则 H 是循环群，它由 F 的所有 n 次单位根构成.

证明 如果 H 的阶为 n，则 H 的任一元素 α 的阶整除 n，因而 α 是一个 n 次单位根，即多项式 x^n-1 的根. 这个多项式最多有 n 个根，故在 F 中没有别的根[第十一章(1.18)]. 于是 H 是 F 中所有 n 次单位根的集合.

证明 H 是循环群比较难. 为此，我们用阿贝尔群的结构定理，它告诉我们 H 同构于一个循环群的直积：

$$H\approx\mathbb{Z}/(d_1)\times\cdots\times\mathbb{Z}/(d_k),$$

其中 $d_1|d_2\cdots|d_k$ 而 $n=d_1\cdots d_k$. 因为 d_k 是所有整数 d_i 的公倍数，所以这个积中每个元素的阶整除 d_k. 因而 H 中每个元素是

$$x^{d_k}-1$$

512

的根. 这个多项式在 F 中最多有 d_k 个根. 但 H 含有 n 个元素而 $n=d_1\cdots d_k$. 仅有的可能性是 $n=d_k$，$k=1$ 且 H 是循环群. ■

定理(6.4a)的证明 我们需要证明存在具有 q 个元素的域. 由于已经证明了定理的(d)，我们知道 q 阶域的元素都是多项式 x^q-x 的根. 而且存在一个包含$\mathbb{F}_q$ 的域L，在其中这个多项式(或任意给定的多项式)分解为线性因式的积(5.3). 自然的方法是试取一个这样的域 L 并期望最好的结果，即 x^q-x 的根构成要求的L 的子域K. 这由下面的命题证明：

513

【6.19】命题 设 p 是一个素数，并设 $q=p^r$.

(a) 在任意特征 p 的域L 中多项式 x^q-x 没有重根.

(b) 设 L 是特征 p 的域，K 是 x^q-x 在 L 中的根的集合. 则 K 是一个子域.

这个命题与命题(5.3)合起来，证明了存在 q 个元素的域. ■

命题(6.19)的证明 (a) x^q-x 的导数为 $qx^{q-1}-1$. 在特征 p 的情形，系数 q 等于 0，因而导数等于-1. 由于常数多项式-1 没有根，因此 x^q-x 与它的导数没有公共根！命题(5.7)表明x^q-x 没有重根.

(b) 设 α，$\beta\in L$ 是多项式 x^q-x 的根，要证明 $\alpha\pm\beta$，$\alpha\beta$ 和 $\alpha^{-1}(\alpha\neq 0)$是同一多项式的根. 积和商是清楚的：如果 $\alpha^q=\alpha$ 和 $\beta^q=\beta$，则$(\alpha\beta)^q=\alpha\beta$ 及$(\alpha^{-1})^q=\alpha^{-1}$. 对于和这是不明显的，我们用下面的命题来证明它：

【6.20】命题 设 L 是特征 p 的域，并设 $q=p^r$. 则在多项式环 $L[x, y]$中，有$(x+y)^q=x^q+y^q$.

证明 先对 $q=p$ 的情形证明命题. 在$\mathbb{Z}[x, y]$中展开$(x+y)^p$，由二项式定理得到

$$(x+y)^p=x^p+\binom{p}{1}x^{p-1}y+\binom{p}{2}x^{p-2}y^2+\cdots+\binom{p}{p-1}xy^{p-1}+y^p.$$

二项式系数$\binom{p}{r}$是整数，且如果$1<r<p$，则它被 p 整除[见第十一章(4.6)的证明]. 由此得到映射$\mathbb{Z}[x, y]\longrightarrow L[x, y]$将这些系数变为零而在 $L[x, y]$中$(x+y)^p=x^p+y^p$.

现在对 r 作归纳来处理一般情形 $q=p^r$：假定命题对小于 r(设 $r>1$)的整数已经证明. 设 $q'=p^{r-1}$. 由归纳法，$(x+y)^q=((x+y)^{q'})^p=(x^{q'}+y^{q'})^p=(x^{q'})^p+(y^{q'})^p=x^q+y^q$. ■

要完成命题(6.19)的证明，我们对 x，y 取值α，β而得到结论$(\alpha+\beta)^q=\alpha^q+\beta^q$. 则如果 $\alpha^q=\alpha$ 及$\beta^q=\beta$，则得到$(\alpha+\beta)^q=\alpha+\beta$，这正是要证的. $\alpha-\beta$的情形由用$-\beta$代入β得到.

定理(6.4b)的证明 设 K 和 K'是 q 阶域，并设α是循环群 $K^\times$ 的生成元. 则 K 当然是由元素α生成的域 $F=\mathbb{F}_p$ 的扩域：$K=F(\alpha)$. 设 f 为α在 F 上的既约多项式，则有 $K\approx F[x]/(f)$ (2.6). 于是α是两个多项式 $f(x)$和 x^q-x 的根. 由于 f 是既约的，它整除 x^q-x(5.4e). 现在看第二个域 K'. 由于 x^q-x 在 K'中分解为线性因子，因此 f 在 K'中有根α'. 于是 $K\approx F[x]/(f)\approx F(\alpha')$. 由于 K 与 K'的阶相同，$F(\alpha')=K'$；因此 K 与 K'同构. ■

514

定理(6.4e)的证明 设 $f(x)$是 $F[x]$中一个 r 次既约多项式，其中像前面一样有 $F=\mathbb{F}_p$. 它在 F 的某个扩域L 中有一个根α，且 L 的子域 $K=F(\alpha)$在 F 上次数为r(3.2). 因而 K 的阶为$q=p^r$，并且由定理之(d)部分，α 亦是 x^q-x 的一个根. 由于 f 是既约的，因此它整除

x^q-x，这正是要证的.

要证明同样的结论对次数 k 整除 r 的既约多项式成立，只需证明下面的引理：

【6.21】引理 设 k 是整除 r 的整数，如设 $r=ks$，并设 $q=p^r$，$q'=p^k$. 则 $x^{q'}-x$ 整除 x^q-x.

因为如果 f 是 k 次既约的，则像上面一样，对任意域 F，在 $F[x]$中 f 整除 $x^{q'}-x$，而后者又整除 x^q-x.

引理的证明 这需要点技巧，因为我们将两次使用等式

【6.22】
$$y^d-1=(y-1)(y^{d-1}+\cdots+y+1).$$

代入 $y=q'$和 $d=s$ 得到 $q'-1$ 整除 $q-1=q'^s-1$. 知道了这一点，就可以通过代入 $y=x^{q'-1}$和 $d=(q-1)/(q'-1)$得到 $x^{q'-1}-1$ 整除 $x^{q-1}-1$. 因而也有 $x^{q'}-x$ 整除 x^q-x. ■

这样就证明了次数整除 r 的每个既约多项式是 x^q-x 的一个因式. 另一方面，如果 f 既约且如果其次数 k 不整除 r，则由于$[K:F]=r$，f 在 K 中没有根，因而 f 不整除 x^q-x.

定理(6.4f)的证明 如果 k 不整除 r，则 $q=p^r$ 不是 $q'=p^k$ 的幂，因而 q 阶域不能是 q'阶域的扩域. 另一方面，如果 k 确实整除 r，则引理(6.21)和定理之(d)部分表明多项式 $x^{q'}-x$ 的所有根属于一个 q 阶域 K. 而现在命题(6.19)表明 K 含有一个 q'元域. ■

这就完成了定理 6.4 的证明.

第七节 函 数 域

本节我们看一下*函数域*，即第一节中提到的第三类扩域. 在整个本节中单变量 x 的有理函数域$\mathbb{C}(x)$将记为 F. 它的元素是多项式 p，$q\in\mathbb{C}[x]$的分式 $g(x)=p(x)/q(x)$，其中 $q\neq0$. 通常消去 p 和 q 的公因式使它们没有公共根.

我们用符号 P 表示复平面，复坐标为 x. 一个有理函数 $g=p/q$ 确定 x 的一个复值函数，它在所有使 $q(x)\neq0$ 的 $x\in P$ 上定义，也就是在除了多项式 q 的根以外的点上定义. 在 q 的一个根附近，由 g 定义的函数趋于无穷. 这些根称为 g 的*极点*. (通常用术语“有理函数”指多项式环的分式域的元素. 遗憾的是这里面已有*函数*一词，这样当提到用这样的分式定义的函数时便不能自然地改动术语. 这个用语是含糊的，但已没有办法改变.) [515]

因为形式有理函数在某些点，也就是在其极点并不定义函数，这就产生了一点小麻烦. 当在整个域 F 上讨论问题时，必须面对这样一个事实：x 的某个值 α 可能是有理函数的一个极点，例如是函数$(x-\alpha)^{-1}$的极点. 没有办法同时为所有的有理函数选择公共定义域. 幸运的是这并不是一个严重的问题，有两个绕过去的办法. 一个是引入额外的值∞并在 g 的极点 α 处定义 $g(\alpha)=\infty$. 这实际上在很多地方都是较好的办法，但另一个办法对我们来说会更为简单. 就是简单地忽略掉在有限点集上的坏行为.

我们要作的任何特定的计算将只会涉及有限多个函数，因而它们在除掉平面 P 上的一个有限集合，也就是这些函数的极点外都将有效. 一个有理函数由它在任意无限点集上的值所确定. 这将在下面的引理(7.2)中加以证明. 因而在必要时，可以从定义域中去掉有限个点而不改变对函数的控制. 由于有理函数只要有定义就是连续的，因此可以恢复不必被去掉的那些点 x_0 上的值为

【7.1】
$$g(x_0)=\lim_{x\to x_0}g(x).$$

【7.2】引理 如果两个有理函数 f_1，f_2 在平面上无限多个点上相同，则它们是 F 中相等的元素.

证明 设 $f_i=p_i/q_i$，其中 p_i，$q_i\in\mathbb{C}(t)$. 设 $h(x)=p_1q_2-p_2q_1$，如果 $h(x)$是零多项式，则 $f_1=f_2$. 如果 $h(x)$不为零，则它仅有有限多个根，因而仅有有限多个点使得$f_1=f_2$. ■

为了直观地提出忽略引起麻烦的有限点集的过程，用一个记号来表示去掉一个有限集后的结果会方便一些. 给定无限集 U，我们将用 U'表示从 U 中删去一个未指定的且必要时可变动的有限子集得到的集合：

【7.3】
$$U'=U-(\text{有限变集}).$$

U'上的一个函数是指复值函数的一个等价类，其中每一个都定义在 U 中除掉一个有限集合外的点上. 两个这样的函数 f，g 称为在U'上相等的，如果存在U 的一个有限子集 Δ 使得 f 和 g 在 $U-\Delta$ 上有定义且相等.（我们也想把这个性质称为在 U 上几乎处处有 $f=g$. 然而在其他地方，“几乎处处”常指“除了一个零测度集以外”，而不是“除了一个有限集以外”.）U'上的函数 f 称为连续的，如果它在某个集合 $U-\Delta$ 上由一个连续函数代表. U'上的连续函数的集合记为

516

【7.4】
$$\mathcal{F}(U)=\{U'\text{ 上的连续函数}\}.$$

这个集合构成一个环，满足函数通常的加法和乘法法则：

【7.5】
$$[f+g](x)=f(x)+g(x),\quad [fg](x)=f(x)g(x).$$

引理(7.2)有下面的推论：

【7.6】命题 域 $F=\mathbb{C}(x)$同构于环$\mathcal{F}(P)$的子环，其中 P 是复平面.

现在更为仔细地考察一个最简单的函数域. 我们需要系数属于域 F 的多项式. 由于符号 x 已被指定了，因此用 y 表示新变量. 我们讨论由在 F 上添加 $f(y)$的一个根得到的二次扩域 K，其中 $f=y^2-x$. 由于 f 依赖于变量 x 及 y，因此也记

【7.7】
$$f=f(x,y)=y^2-x.$$

多项式 y^2-x 是 $F[y]$的一个既约元，因而 K 可以作为抽象域 $F[y]/(f)$构造出来. 变量 y 的剩余是 f 在 K 中的根.

函数域的重要性在于其元素可以解释为实际的函数这个事实. 在我们的情形中，通过选定每个复数 x 的平方根的两个值中的一个：$h(x)=\sqrt{x}$，可以定义平方根函数 h. 则 h 可以解释为 P'上的一个函数. 然而当 $x\neq 0$ 时，平方根有两个值，我们需要作很多选择来定义这个函数. 这不能令人满意. 如果 x 是正实数，则选择正平方根是自然的，但在整个复平面上没有能够给出连续函数的选择.

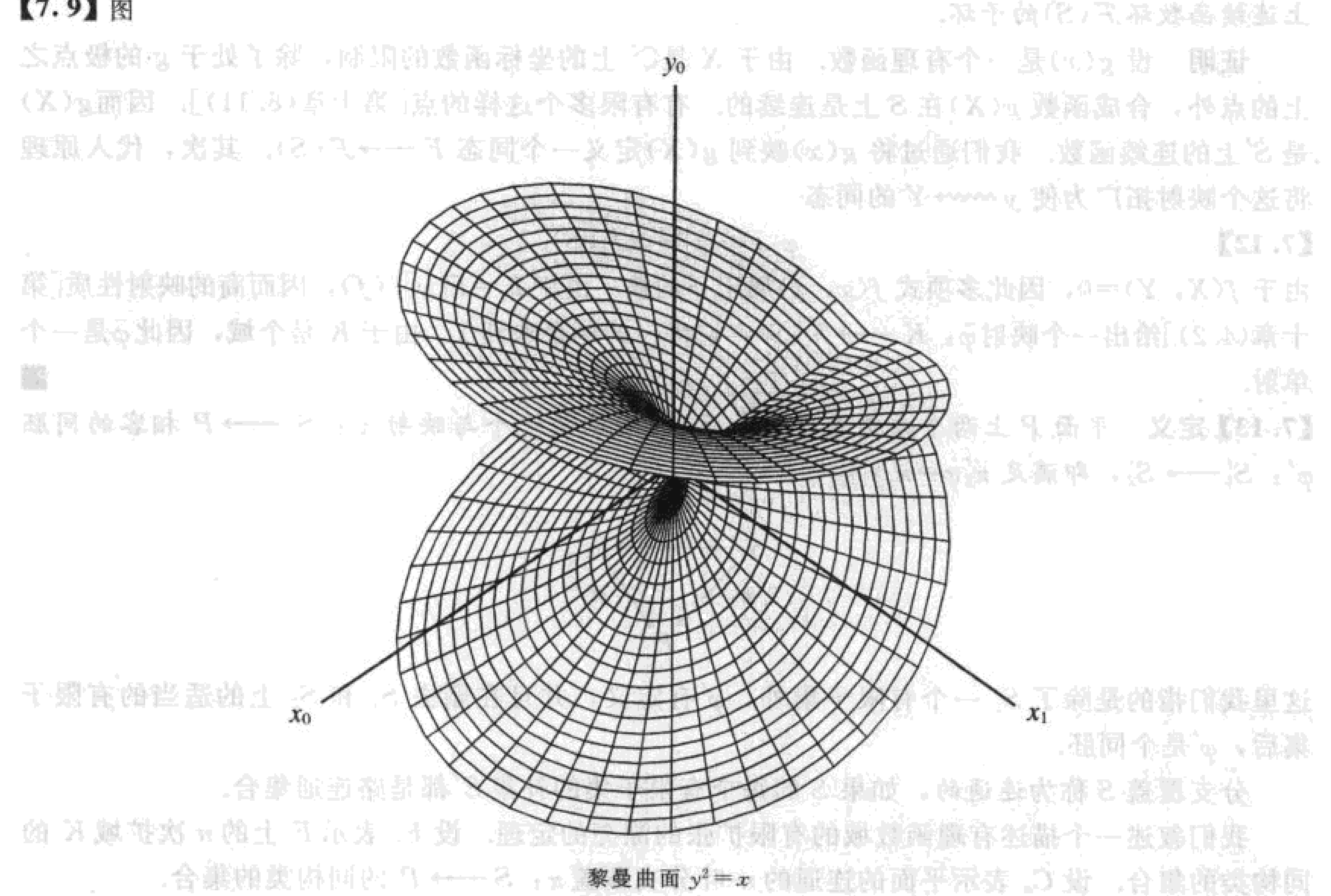
方程 $y^2-x=0$ 在$\mathbb{C}^2$ 的解的轨迹 S 称为多项式 y^2-x 的黎曼曲面(见第十章第八节). 如下图(7.9)所示，但为了在实 3-空间中得到曲面，我们去掉一个坐标. 按通常的规则$(x, y)=(x_0+x_1\mathrm{i}, y_0+y_1\mathrm{i})\leftrightarrow(x_0, x_1, y_0, y_1)$，复二维空间$\mathbb{C}^2$ 等同于$\mathbb{R}^4$. 图描绘了轨迹

【7.8】
$$\{(x_0,x_1,y_0)\mid y_0=(x_0+x_1\mathrm{i})^{1/2}\text{ 的实部}\}.$$

517

它是 S 从$\mathbb{R}^4$ 到$\mathbb{R}^3$ 的投影.

【7.9】图



黎曼曲面 $y^2=x$

黎曼曲面 S 并不像投射的象那样沿负 x 轴切除自身. 每一个负实数 x 有两个纯虚平方根，但这些平方根的实部都为零. 这产生了投影曲面显现出来的自相交. 事实上，如第十章(8.13)所示，S 是 P 的两叶分支覆盖，其仅有的分支点在 $x=0$ 处.

图(7.9)显示了当试图将平方根定义为单值函数时遇到的问题. 当 x 为正实数时，正平方根是自然的选择. 我们想要连续地将这个选择拓广到复平面，于是就陷进了麻烦中：在复 x-空间绕原点转一次把我们带回到负平方根. 最好是接受下面的事实：作为 y^2-x 的解，平方根是 P' 上的一个多值函数.

有一个令人称奇的技巧，它使我们能够用一个单值函数来解任意多项式方程 $f(x, y)=0$ 而不需作任意的选择. 诀窍就是用黎曼曲面 S，也就是 $f(x, y)=0$ 的轨迹来代替复平面 P. 在 S 上给定了两个函数，即 $\mathbb{C}^2$ 上的坐标函数的限制. 为保持一切顺畅，我们对这些函数引入新的记号，如 X，Y： 518

【7.10】 $$X(x,y)=x \quad 及 \quad Y(x,y)=y, \quad 对所有 \quad (x,y)\in S.$$

坐标函数在 S 上的这些限制通过方程 $f(X, Y)=0$ 相联系，这是因为由定义，在 S 上的任意点有 $f(x, y)=0$.

【7.11】命题 设 $f(x, y)$ 是 $\mathbb{C}[x, y]$ 中的既约多项式，且不是单独一个 x 的多项式，并设 $S=\{(x, y) \mid f(x, y)=0\}$ 是其黎曼曲面. 设 $K=F[y]/(f)$ 是 f 定义的扩域. 则 K 同构于 S'

上连续函数环$\mathcal{F}(S)$的子环.

证明 设$g(x)$是一个有理函数. 由于X是$\mathbb{C}^2$上的坐标函数的限制，除了处于g的极点之上的点外，合成函数$g(X)$在S上是连续的. 有有限多个这样的点[第十章(8.11)]. 因而$g(X)$是S'上的连续函数. 我们通过将$g(x)$映到$g(X)$定义一个同态$F \longrightarrow \mathcal{F}(S)$. 其次，代入原理将这个映射拓广为使$y \rightsquigarrow Y$的同态

【7.12】
$$\varphi: F[y] \longrightarrow \mathcal{F}(S).$$
由于$f(X, Y)=0$，因此多项式$f(x, y)$属于φ的核. 由于$K=F[y]/(f)$，因而商的映射性质[第十章(4.2)]给出一个映射$\overline{\varphi}$: $K \longrightarrow \mathcal{F}(S)$，它将$y$的剩余映到$Y$. 由于$K$是个域，因此$\overline{\varphi}$是一个单射. ■

【7.13】定义 平面P上两个分支覆盖S_1，S_2的同构是一个与映射π_i: $S_i \longrightarrow P$相容的同胚φ': $S_1' \longrightarrow S_2'$，即满足$\pi_2'\varphi=\pi_1'$:

$$\begin{array}{ccc} S_1' & \xrightarrow{\varphi'} & S_2'. \\ & {\scriptstyle\pi_1'}\searrow \quad \swarrow{\scriptstyle\pi_2'} & \\ & P & \end{array}$$

这里我们指的是除了S_1一个有限子集外，φ'有定义，并且在删去S_1和S_2上的适当的有限子集后，φ'是个同胚.

分支覆盖S称为连通的，如果S的每个有限子集的补集S'都是路连通集合.

我们叙述一个描述有理函数域的有限扩张的漂亮的定理. 设E_n表示F上的n次扩域K的同构类的集合. 设C_n表示平面的连通的n-叶分支覆盖π: $S \longrightarrow P$的同构类的集合.

【7.14】定理 黎曼存在定理：存在一个一一映射Φ_n: $\mathscr{E}_n \longrightarrow \mathscr{C}_n$. 如果$K$是由添加既约多项式$f(x, y) \in \mathbb{C}[x, y]$的一个根得到的一个扩张，则对应于$K$的分支覆盖的类由$f$的黎曼曲面代表. ■

519

这个定理的证明是复分析课程的一个适当的课题. 它需要的分析太多而不可能在这里给出. 然而，应用这个定理，我们可以将F上的每个有限扩域K在同构下用唯一的平面的分支覆盖与之对应. 这个覆盖称为扩域K的黎曼曲面. F的黎曼曲面本身是一个复平面P.

下面是这个定理的两个重要推论.

【7.15】推论 给定平面上一个连通的n-叶分支覆盖，存在y的一个n次多项式$f(x, y)$，其黎曼曲面同构于S.

这由映射Φ_n是满射和在下一章证明的F的每个有限扩域K可以由添加单独一个元素得到这样一个事实[第十四章(4.1)]得到.

【7.16】推论 如果f，g是$\mathbb{C}[x, y]$的既约多项式，其黎曼曲面为S，T. 设α是$f(y)$在F的一个扩域中的根. 如果S，T是同构的分支覆盖，则$g(y)$在$F(\alpha)$中有一个根.

这由映射Φ_n是单射得到.

黎曼曲面的可视化是很复杂的，这是因为黎曼曲面所嵌入的$\mathbb{C}^2$是一个实的4维空间. 构造和可视化它们的一个辅助方法是称为剪贴的方法. 如果沿负实轴切开曲面y^2-x，也就是图(7.9)中的重合轨迹，则它分解为两部分re $Y>0$和re $Y<0$. 如果忽略切口上发生了什么，则这两部分

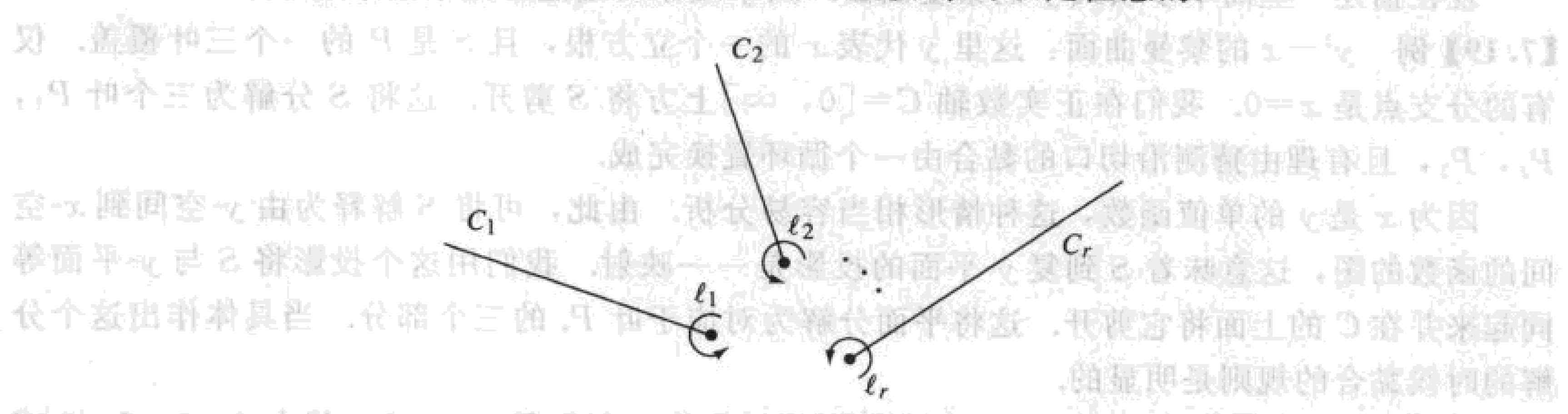
的每一个都以双射的方式投射到 x-平面 P 上. 将这个过程翻转过来，可以用下面的方法构造一个与 S 同胚的曲面：将 P 上两个复平面的副本叠起来并将它们沿负实轴 $(-\infty, 0]$ 剪开. P 的这些副本称为叶. 然后将 P_1 的 A 边与 P_2 的 B 边粘起来，反之亦然(见下面). 要把 S 不相交地嵌进去需要四维.

【7.17】图

$$\frac{\text{前切口的 } A \text{ 边}}{\text{剪切口的 } B \text{ 边}}.$$

要用剪贴的方法构造平面一般的分支覆盖 S，我们从平面的 n 个称为叶的副本开始. 将这些叶标为 P_1，…，P_n 且叠在 P 之上. 还要选择 P 上有限个点的集合 α_1，…，α_r 作为分支点. 对每个分支点 α_ν，选取一条从 α_ν 开始并从任意方向走向无穷远的曲线. 选择的方式应该使得这些曲线 C_ν 互不相交. 叶 P_i 沿这些曲线剪开，不同的叶沿着剪口的对边与其他叶粘贴起来. 520

为描述得到的覆盖 S，只需要描述使叶沿剪口粘起来的置换 σ_ν. 更具体一点，我们绕点 α_ν 以反时针方向画一个圈 ℓ_ν. 如果置换 σ_ν 将指标 **1** 变到 **3**，则当穿过 C_ν 时，把 P_1 粘贴到 P_3. 这是说当从 P_1 出发而绕圈 ℓ_ν 转一圈，我们回到 P_3. 置换 σ_ν 可以是任意的.



点 α_ν 称为曲面 S 的分支点，这是因为在 P 的任何其他点附近曲面分解为 n 个不相交的叶. 除非置换 σ_ν 是恒等的，否则在点 α_ν 附近不会有 n 个不相交的叶. 如果 $\sigma_\nu=1$，则每个页沿剪口 C_ν 与自己贴合，因而剪开是不必要的. 但允许这作为剪贴的一种可能是方便的. 我们称 α_ν 为一个真分支点，如果 $\sigma_\nu \neq 1$. 点 α_ν 中的一些可能不是真的分支点. 然而，所有真的分支点都一定在其中.

重要的是要注意叶的编号可以是任意的，特别地，"顶层"的概念对多项式的黎曼曲面没有本质的意义. 如果存在顶层，则可以通过选择在该层的值而定义 y 为一个单值函数. 只有在黎曼曲面被切开时才能这样做. 这是整个的要点：在曲面上漫步将使我们从一叶走到另一叶.

不难确定什么时候两个这样的分支覆盖是同构的.

【7.18】命题 设 S，T 是如上面构造的分支覆盖，有相同的分支点 α_ν 和相同的曲线 C_ν，但有不同的置换集合 $(\sigma_1, \cdots, \sigma_r)$ 和 $(\tau_1, \cdots, \tau_r)$. 则 S 和 T 是同构的覆盖当且仅当两个置换的集合是共轭的，即当且仅当存在一个置换 ρ 使得对所有 ν 有 $\tau_\nu=\rho^{-1}\sigma_\nu\rho$. 521

证明 设 σ，C 表示 σ_ν，C_ν. 我们的规则是沿 C 将 P_i 粘贴到 $P_{i\sigma}$. 假定重新对叶 P_1，…，P_n 标号，通过置换 ρ 改变数字. 为保持旧的和新的标号一致，我们把重新标的页记作 Q_j. 于是对每个 i，P_i 重新标为 $Q_{i\rho}$. 规则告诉我们将 $P_i=Q_{i\rho}$ 与 $P_{i\sigma}=Q_{i\sigma\rho}$ 粘贴起来. 代入 $i=j\rho^{-1}$ 表明规则

将 Q_j 与 $Q_{j\rho^{-1}\varphi}$ 粘贴起来．这样描述这个粘贴规则的置换是原有置换 σ_ν 的共轭 $\rho^{-1}\sigma_\nu\rho$．由于重新标号过程没有改变覆盖，这就证明了置换的共轭集合定义了同构的覆盖．

反之，设 $\varphi:S\longrightarrow T$ 是覆盖的一个同构．设 P_1，…，P_n 是用来构造覆盖 S 的叶，并设 Q_1，…，Q_n 是用来构造覆盖 T 的叶．则由于 P_i 是连通的而 T 在剪开时是开集 Q_j 的不相交并，因此 P_i 的象必须包含在单独一个叶 Q_j 之中．由于 φ 与到 P 的投射相容，而它除了在切口上之外是同胚，因为 φ 在 P_i 的限制必为到叶 Q_j 的一一映射．我们可以重新标号叶 Q_j 使 P_i 映到 Q_i．像上面一样，这使置换 τ_ν 变为其共轭．因而可以假设 φ 将 P_i 映到 Q_i．还有，φ 过剪口是连续的．因而如果经过剪口从叶 P_i 到 P_j，则类似地也经过剪口从 Q_i 到 Q_j．因而 $\sigma_\nu=\tau_\nu$． ■

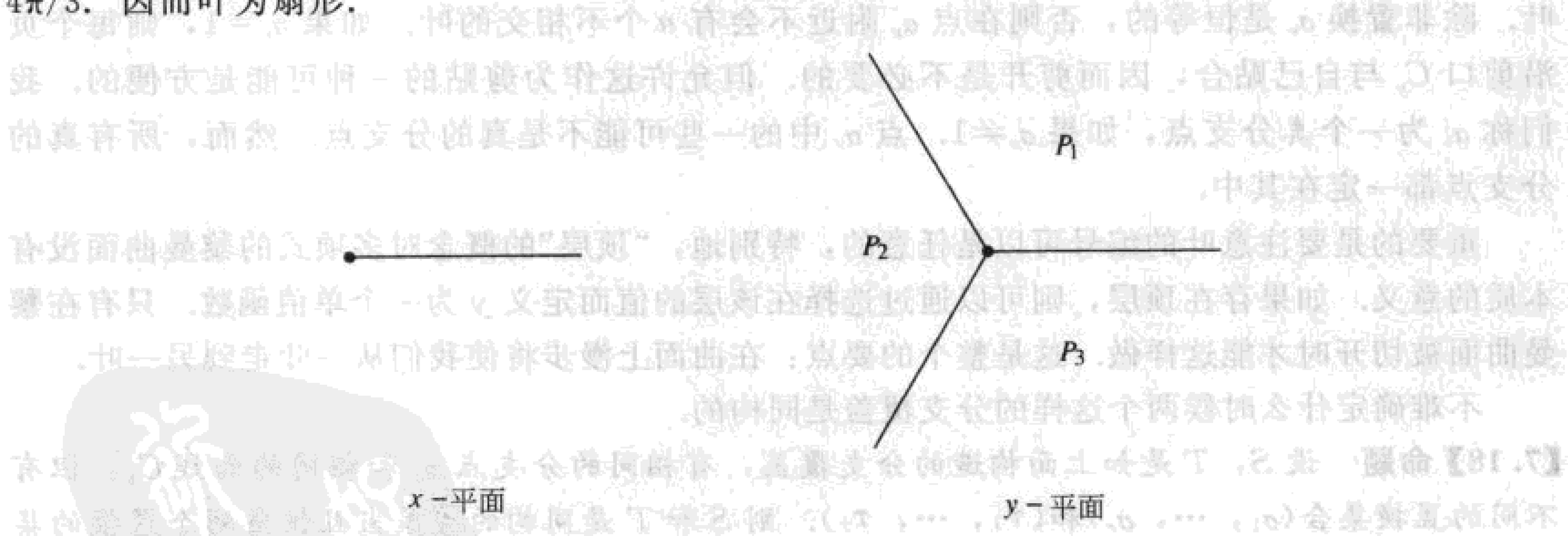
我们也可以用这样的方法从任意的分支覆盖 S 开始并重新构造它：比如 S 是在点 α_1，…，$\alpha_r\in P$ 处的分支覆盖．和上面一样，选取从 α_i 开始到无穷远的互不相交的曲线 C_i．则如果 S 在曲线 C_i 的上方剪开，它分解成 n 个叶．这是一个拓扑的定理，因为 P 中曲线 C_i 的补集合是单连通的[Munkres，*Topology* p. 342，exc. 8]．因而与 S 同胚的覆盖可由 n 叶 P_1，…，P_n 通过沿曲线剪开并黏合起来以将叶混合而构造出来．

现在描述一些简单多项式 f 的黎曼曲面．当 f 复杂时这通常是很困难的．

【7.19】例 y^3-x 的黎曼曲面：这里 y 代表 x 的一个立方根，且 S 是 P 的一个三叶覆盖．仅有的分支点是 $x=0$．我们在正实数轴 $C=[0,\infty]$上方将 S 剪开．这将 S 分解为三个叶 P_1，P_2，P_3，且有理由猜测沿切口的黏合由一个循环置换完成．

因为 x 是 y 的单值函数，这种情形相当容易分析．由此，可将 S 解释为由 y-空间到 x-空间的函数的图，这意味着 S 到复 y-平面的投影是一一映射．我们用这个投影将 S 与 y-平面等同起来并在 C 的上面将它剪开．这将平面分解为对应于叶 P_i 的三个部分．当具体作出这个分解的时候黏合的规则是明显的．

y 在切口 C 上的值是使 $y^3=x$ 为正实数的那些值．它们是 $y=re^{i\theta}$，其中 $\theta=0$，$2\pi/3$ 或 $4\pi/3$．因而叶为扇形．

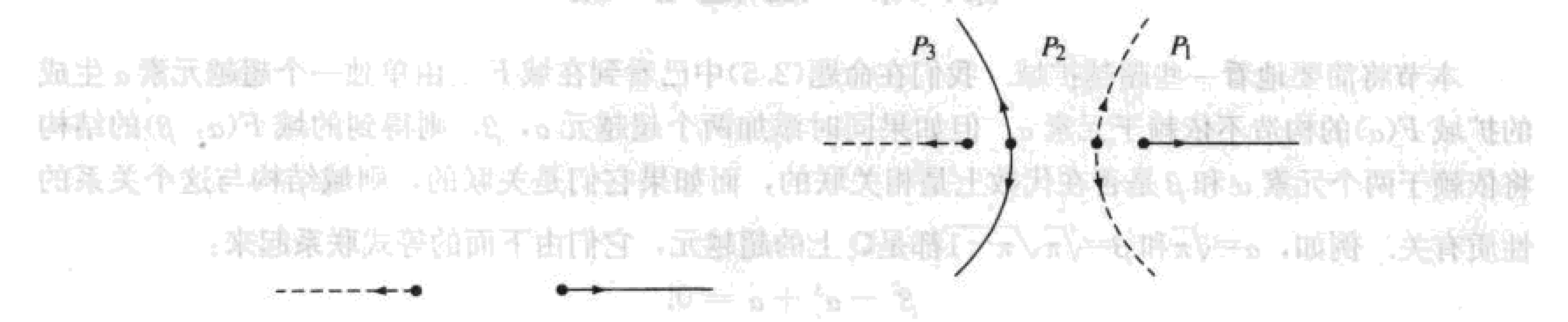


图中扇形的标号是任意的．注意在映射 $y \rightsquigarrow y^3=x$ 下，如果不考虑切口，三个扇形中的每一个放射性地伸展开来且都一一地映射到整个平面．当沿着 S 穿过 x-平面的切口时，也穿过 y-平面上的三个切口之一．正如我们所预测的，这通过循环置换(**123**)置换了叶．

【7.20】例 黎曼曲面 $f(x,y)=y^3-3y-x$：通过解方程 $f=\partial f/\partial y=0$ 求得使多项式有少于三

个根的点 x[见第十章(8.12)]．这里$\partial f/\partial y=3(y^2-1)$．因而解为 $y=\pm1$，因此 $x=\pm2$．我们可以在曲线 $C_1=(-\infty,\ -2]$和 $C_2=[2,\ \infty)$上面剪开 S 而将它分解为三个叶．

x 也是 y 的单值函数，而且可以通过适当地将 y-平面剪开来分析叶的黏合．为此要求当 x 在曲线 C_i 之一上时 y 的值．由于这些曲线在实 x-轴上，因此从解方程 $\mathrm{im}x=0$ 开始．取 $y=u+vi$，我们得到 $\mathrm{im}x=\mathrm{im}(y^3-3y)=v(3u^2-v^2-3)$．解是 u-轴 $v=0$ 及双曲线$3u^2-v^2=3$ 的两个分支．在 u 轴上区间$(-2,\ 2)$中的点对应于 $x\in(-2,\ 2)$，因而它们不位于剪口的上面．



523

我们还是像往常一样忽略剪口，则 y-平面所分解成的三个区域的每一个也由函数 y^3-3y 一一地映到 x-平面上．上图中，有点的曲线位于 C_1 上．该图表明在 S 上移动穿过曲线$(-\infty,\ -2]$交换两叶 P_1，P_2，单独留下 P_3，而类似地，穿过曲线$[2,\ \infty)$交换 P_2，P_3．因而在分支点 $x=-2$ 处分支由对换(**23**)描述而在 $x=2$ 处由对换(**12**)描述．

【7.21】例　黎曼曲面 $y^2-x^3+x^2$：存在两个点 $x=0$，1，在其上 S 有少于两个点．然而在 $x=0$处两叶相交而未重合，因而真正的分支点是 $x=1$．为此我们作除了在 $x=0$ 点以外都有定义且可逆的变量代换 $x=x$，$z=y/x$．则 $z^2-x+1=0$．给定的曲面 S 成为当删除原点上面的点后与 z^2-x+1 同胚的黎曼曲面，而这个曲面可以通过在 x-平面上的平移化简为(7.9)．

当 x 不能作为 y 的单值函数解出时，描述黏合数据的问题就变得更为复杂．我们将给出一个这样的例子．

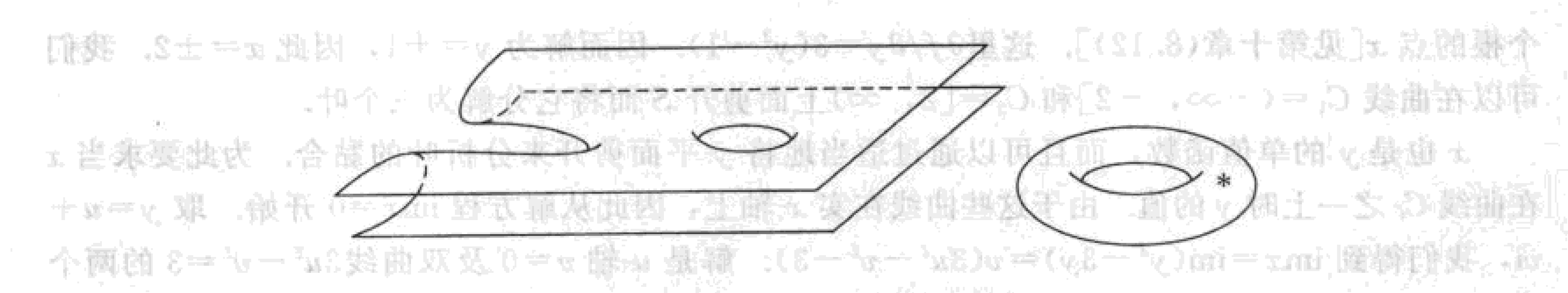
【7.22】例　黎曼曲面 $y^2-(x^3-x)$：存在三个使得 $x^3-x=0$ 的点，即 $x=0$，±1，且曲面有三个分支点，在这些点上的性质就像黎曼曲面 y^2-x 在原点一样．系统的做法是作从这三个分支点到无穷远点的剪口，但在这种情形下另外的剪口更容易分析．使得 y 为纯虚数的 x 的值是使得 $x^3-x<0$ 的实数 x．它们是两个区间$(-\infty,\ -1]$和$[0,\ 1]$中的点．如果沿这两个区间将 S 剪开，它将分解为 $\mathrm{re}y>0$ 和 $\mathrm{re}y<0$ 两部分．这样可以通过将 P 的两个副本叠起来，沿这两个区间将它剪开，并像前面那样黏合两个叶而重新构造 S．

【7.23】图

-1　　0　　1

通过剪贴方法构造的曲面沿剪口穿过自身这一事实使得不好作图示．但在这个例子里由于是沿实轴剪切，因此可以将其中一叶翻转过来而避免穿过自身．这破坏了 S 作为 P 的双重覆盖的表示，但有着沿剪口的同边黏合的优势．在图(7.23)中有两个这样的剪口．将其中一叶翻转过来在黏合后使之拉伸展开得到下面的图：黎曼曲面与去掉一个点的环面同胚．

524



第八节 超越扩域

本节将简要地看一些超越扩域．我们在命题(2.5)中已看到在域F上由单独一个超越元素α生成的扩域$F(\alpha)$的构造不依赖于元素α．但如果同时添加两个超越元α，β，则得到的域$F(\alpha,\beta)$的结构将依赖于两个元素α和β是否在代数上是相关联的，而如果它们是关联的，则域结构与这个关系的性质有关．例如，$\alpha=\sqrt{\pi}$和$\beta=\sqrt[4]{\pi}\sqrt{\pi-1}$都是$\mathbb{Q}$上的超越元，它们由下面的等式联系起来：

$$\beta^2-\alpha^3+\alpha=0.$$

一般地，扩域$K\supset F$的元素集$\{\alpha_1,\cdots,\alpha_n\}$称为在$F$上是代数相关的，如果存在非零的$n$元多项式$f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$，使得

$$f(\alpha_1,\cdots,\alpha_n)=0,$$

而称它们在F上是代数无关的，如果没有这样的多项式存在．这样$\alpha=\sqrt{\pi}$和$\beta=\sqrt[4]{\pi}\sqrt{\pi-1}$在$\mathbb{Q}$上是代数相关的．有一个猜想说$\pi$和e是代数无关的，但至今还没有得到证明．

我们可以用使$f(x_1,\cdots,x_n)\rightsquigarrow f(\alpha_1,\cdots,\alpha_n)$的代入同态$\varphi:F[x_1,\cdots,x_n]\longrightarrow K$的语言解释代数无关性．元素$\alpha_1,\cdots,\alpha_n$是代数无关的，如果$\ker\varphi=0$，即$\varphi$是单射，否则就是代数相关的．放到分式域上给出下面的命题：

【8.1】命题 *如果$\alpha_1,\cdots,\alpha_n$是代数无关的，则$F(\alpha_1,\cdots,\alpha_n)$同构于$x_1,\cdots,x_n$的有理函数域$F(x_1,\cdots,x_n)$，也就是$F[x_1,\cdots,x_n]$的分式域．*

一个形如$F(\alpha_1,\cdots,\alpha_n)$的扩域(其中$\alpha_i$代数无关)称为一个纯超越扩域．

【8.2】定义 *F的扩域K的一个超越基是一个代数无关的元素集合$(\alpha_1,\cdots,\alpha_n)$，并且使得$K$是域$F(\alpha_1,\cdots,\alpha_n)$的代数扩张．*

525

【8.3】定理 *设$(\alpha_1,\cdots,\alpha_m)$和$(\beta_1,\cdots,\beta_n)$为一个域$F$的扩域$K$的元素．假定$K$在$F(\beta_1,\cdots,\beta_n)$上是代数的，且$\alpha_1,\cdots,\alpha_m$在$F$上是代数无关的．则$m\leqslant n$，且可通过添加$\beta_i$中的$n-m$个元素而将$(\alpha_1,\cdots,\alpha_m)$补齐为$K$的超越基．*

我们将这个定理的证明留作练习．

【8.4】推论 *一个扩张$F\subset K$的任意两个超越基有相同数量的元素．*

【8.5】定义 *K的超越次数是一个超越基中元素的个数，而如果没有有限超越基时它为无限．*

【8.6】例

(a) 对于不同的n值，n个变量的有理函数域$F(x_1,\cdots,x_n)$互不同构，因为$(x_1,\cdots,x_n)$是超越基．

(b) 设α，β如本节开头给出．单独一个元素π构成$K=\mathbb{Q}(\alpha,\beta)$在$\mathbb{Q}$上的超越基．因而(8.3)蕴涵$K$中任意两个元素是代数相关的，这正如前面所断言的．元素β是另一个超越基．

(c) 考虑一个变量的任意两个多项式或有理函数 f，$g\in F(x)$. 存在一个非零多项式 $\varphi(y, z)\in F[y, z]$使得 $\varphi(f, g)=0$. 这是因为 $F(x)$的超越次数为 1，因此 f，g 是代数相关的.

大多数扩域都不是纯超越的，虽然对特定的扩域难于确定它是否是纯超越的. 下面是两个例子：

【8.7】命题

(a) 函数域 $L=\mathbb{C}(x)[y]/(y^2-x^3)$是$\mathbb{C}$的纯超越扩张. 它是 $t=y/x$ 的有理函数域.

(b) 函数域 $K=\mathbb{C}(x)[y]/(y^2-x^3+x)$不是$\mathbb{C}$的纯超越扩张. 即没有元素 $t\in K$ 使得 $K=\mathbb{C}(t)$.

证明 在这两种情形下，K 在$\mathbb{C}$上的超越次数都是 1，因为 x 是一个超越基.

(a) 设 $t=y/x$. 则因为 $t\in L$，所以有$\mathbb{C}(t)\subset L$. 由定义，L 是由 x 和 y 生成的. 另一方面，$x=t^2$ 而 $y=t^3$. 因而 $L=\mathbb{C}(t)$. 由于 K 的超越次数为 1，(8.4)表明 t 是超越的.

(b) (概要)要证 K 不是有理函数域，我们求助于其黎曼曲面的几何. 在上一节看到这个曲面是环面删去一个点. 另一方面，有理函数域$\mathbb{C}(t)$的黎曼曲面是复平面自身. 环面和平面不同胚并且当删去它们的有限个点后也不会同胚，这是一个拓扑学的定理. 如果我们承认这个定理，则下面的命题将完成证明.

526

【8.8】命题 设 $K=\mathbb{C}(x)[y]/(f)$及 $L=\mathbb{C}(t)[u]/(g)$是函数域，其黎曼曲面分别为 S，T. 一个在子域$\mathbb{C}$上为恒等的同态 $\varphi: L\longrightarrow K$ 导出一个在除了一个有限点集以外的点上有定义且连续的黎曼曲面之间的映射 $\varphi^*: S'\longrightarrow T$. 如果 φ 是一个同构，则当在 S 和 T 上删掉适当的有限集合后，φ^* 成为一个同胚.

注意映射 φ^* 从 K 的黎曼曲面映到 L 的黎曼曲面，与 φ 的方向相反.

证明 黎曼曲面 T 是$\mathbb{C}^2$ 中的轨迹 $g(t, u)=0$. 根据命题(7.11)，每个元素 $\alpha\in K$ 定义 S' 上的一个连续函数，因而一对函数$(\varphi(t), \varphi(u))$定义一个连续映射 $S'\longrightarrow\mathbb{C}^2$. 由于在 L 中 $g(t, u)=0$ 且由于 φ 是使 g 的系数不变的同态，因而也有 $g(\varphi(t), \varphi(u))=0$. 因此 S'映到 T. 这就是要求的映射 φ^*. 如果 φ 是同构，其逆定义一个映射 $T'\longrightarrow S$，它在一个有限集合的补集上是 φ^* 的逆函数. ■

第九节 代数闭域

域 F 称为代数闭的，如果每个正次数多项式 $f(x)\in F[x]$在 F 中有一个根. 复数域$\mathbb{C}$是代数闭域这个事实称为代数基本定理.

【9.1】定理 代数基本定理：每个非常数复系数多项式有一个复根.

我们经常用到这个定理. 本节的最后给出它的一个证明.

如果一个域 F 是代数闭的，则每个非常数多项式 $f(x)\in F[x]$有一个线性因子 $x-\alpha$，因而仅有的既约多项式是线性的. 于是每个多项式是线性因子的乘积. 而且除了 F 本身以外没有其他代数扩域(代数闭这个术语就是由此得来的). 因为如果 α 在 F 上是代数的，则它是一个首一既约多项式 $f(x)\in F[x]$的根. 这个多项式必有 $x-\alpha$ 的形式，因而 $\alpha\in F$.

将所研究的域视为代数闭域的子域会很方便. 例如我们喜欢把数域看作复数域$\mathbb{C}$的子域. 我们把 F 的一个扩域 K 称为 F 的代数闭包，如果

【9.2】

(i) K 在 F 上是代数的，且

527 (ii) K 是代数闭的.

【9.3】推论 设 F 是$\mathbb{C}$的子域. 则由 F 上的所有代数元组成的$\mathbb{C}$的子集 $\overline{F}$ 是 F 的代数闭包.

证明 $\overline{F}$ 是一个域这一事实已经在(3.10)中证明. 要证 $\overline{F}$ 是代数闭的，设 $f(x)\in\overline{F}[x]$是一个非常数的多项式. 则 $f(x)$在$\mathbb{C}$中有一个根 α，且 $\overline{F}(\alpha)$在 $\overline{F}$ 上是代数的. 由于$\overline{F}$ 在 F 上是代数的，由(3.11)，α 在 F 上是代数的. 因而$\alpha\in\overline{F}$. ■

不难构造有限域$\mathbb{F}_p$ 的代数闭包，取作域$\mathbb{F}_q$ 的并，其中 $q=p^r$ 是 p 的一个幂. 为此，我们选择整数序列 r_1，r_2，…使之具有下列性质：(i)r_i 整除 r_{i+1}，(ii)每个整数 n 整除某个 r_i. 例如可取 $r_i=i!$. 令 $q_i=p^{r_i}$和 $F_i=\mathbb{F}_{q_i}$. 由(i)得到 F_{i+1}包含一个同构于 F_i 的子域(6.4)，因而可以构造一个子域链 $F_1\subset F_2\subset\cdots$. 设 $\overline{F}$ 为这个域链的并. 而(ii)告诉我们每个有限域$\mathbb{F}_q$，$q=p^r$同构于某个 F_i 的子域，因此同构于 $\overline{F}$ 的子域. 这个域是$\mathbb{F}_p$ 的代数闭包.

用佐恩引理可以证明下面的定理.

【9.4】定理 每个域 F 有代数闭包，且如果 K_1，K_2 都是 F 的代数闭包，则存在一个在子域 F 上为恒等映射的同构 $\varphi:K_1\longrightarrow K_2$.

这样代数闭包在本质上是唯一的.

【9.5】推论 设 $\overline{F}$ 是 F 的代数闭包，并设 K 是 F 的任意代数扩域. 存在一个同构于 K 的子扩域 $K'\subset\overline{F}$.

代数基本定理的证明 要证 $f(x_0)=0$，只需证明绝对值 $|f(x_0)|$ 为零. 这样的值 $x_0\in\mathbb{C}$的存在性由下面两个引理证明：

【9.6】引理 设 $f(x)$是一个非常数多项式，并设 $x_0\in\mathbb{C}$是使得 $f(x_0)\neq0$ 的点. 则 $|f(x_0)|$ 不是 $|f(x)|$ 的极小值.

【9.7】引理 设 $f(x)$是个复多项式. 则 $|f(x)|$ 在某个点 $x_0\in\mathbb{C}$取得极小值.

引理(9.6)的证明 我们首先注意到对于所有 $c\in\mathbb{C}$ 多项式 x^k-c 有一个根. 因为当 $x=0$时连续函数 x^k 为零而当 x 为大实数时它也很大，由中值定理，它取到所有$\geqslant0$ 的实数，因而一个非负实数 r 有一个 k 次实根. 将复数 c 记为 $c=re^{i\theta}$的形式，其中 $r=|c|$ 而 $\theta=\arg c$. 设 s是 r 的一个实 k 次根. 则所要求的 c 的 k 次根为

【9.8】
$$\alpha = se^{i\theta/k}.$$

现在设 $f(x)$是个非常数多项式，并设 $x_0\in\mathbb{C}$是使得 $f(x_0)\neq0$ 的点. 将 f 正规化后再做会

528 方便些. 作变量变换，用 $x+x_0$ 代替 x 而将所讨论的点移到原点：$x_0=0$. 用 $f(0)^{-1}$乘 $f(x)$使得 $f(0)=1$，因而必须证明 1 不是 $|f(x)|$ 的极小值.

设 k 表示 x 在 f 中出现的最低非零次幂，因而有

$$f(x) = 1 + ax^k + (\text{次数} > k \text{ 的项}).$$

设 α 为$-a^{-1}$的一个 k 次根，再作最后一次变量代换，用 αx 代替 x. 则对某个多项式$g(x)$，f具有

$$f(x) = 1 - x^k + (\text{高次项}) = 1 - x^k + x^{k+1}g(x)$$

的形式. 对于小的正实数 x，由三角形不等式得到

$$|f(x)|\leqslant|1-x^k|+|x^{k+1}g(x)|=1-x^k+x^{k+1}\ |g(x)|=1-x^k(1-x\,|g(x)|).$$

由于对很小的 x，$x\,|g(x)|$ 也很小，因此当 x 为充分小的正实数时 $x^k(1-x\,|g(x)|)$是正的. 对于这样的 x，有 $|f(x)|<|f(0)|$. ■

引理(9.7)的证明 可假设 $f(x)$不是常数多项式. 对于大的 x，$f(x)$也很大：

【9.9】 当 $x\longrightarrow\infty$ 时 $|f(x)|\longrightarrow\infty$.

要证这一点，f 的常数项是无关紧要的，因而可假设它为零. 于是 $f(x)$ 被 x 整除：$f(x)=xg(x)$. 对次数作归纳，如果 $g(x)$不是常数，断言对 $g(x)$成立，因而断言对 $f(x)$也成立.

现在由于对很大的 x，$f(x)$也很大，$|f(x)|$ 在整个复平面上的最大下界也是在一个充分大的圆盘 $|x|\leqslant r$ 上的最大下界. 由于圆盘是紧的而 $|f(x)|$ 是连续函数，则它在圆盘上取到极小值. ■

代基本定理有几个其他的证明，其中之一特别引人注目，虽然它不像刚才这个这样容易准确地给出. 我们将对它做一个概述. 像前面一样，我们的问题是证明非常数多项式

【9.10】 $$f(z)=z^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0$$

有一个根. 如果 $a_0=0$，则 0 是一个根，因而可以假设 $a_0\neq0$. 考虑由多项式(9.10)定义的函数 f：$\mathbb{C}\longrightarrow\mathbb{C}$.

设 C_r 表示以原点为圆心，r 为半径的圆. 我们研究圆 C_r 的象 $f(C_r)$. 为此，采用极坐标，记 $z=re^{i\theta}$. 则 $z^n=r^ne^{in\theta}$. 当 θ 从 0 转到 2π，点 z 绕半径为 r 的圆转一圈. 同时 $n\theta$ 从 0 转到 $2n\pi$，因而点 z^n 绕半径为 r^n 的圆转 n 圈.

对充分大的 r，项 z^n 控制了表达式(9.10)，我们将有

$$|f(z)-z^n|\leqslant\frac{1}{2}r^n.$$

529

这一事实的证明与引理(9.6)的证明类似. 对于我们来说，因子$\frac{1}{2}$可以用任何小于 1 的正实数代替. 这个不等式表明，随着 z^n 绕半径为 r^n 的圆转 n 圈，$f(z)$也绕原点转了 n 圈. 图示这个结果的一个很好的办法是牵狗模型. 如果一个人绕一个街区溜狗走了 n 圈，则狗也走了 n 圈，虽然路线不一样. 如果拴狗的皮带的长度比街区的半径小这就是对的. 这里 z^n 代表人在时间 θ 的位置，而 $f(z)$代表狗的位置. 皮带的长度是$\frac{1}{2}r^n$.

现在变动半径 r. 由于 f 是连续函数，象 $f(C_r)$将随 r 连续地变化. 当半经非常小时 $f(C_r)$成为一个绕 f 的常数项 a_0 的一个小圈. 这个小圈可以根本不绕原点. 但如我们刚看到的那样，如果 r 足够大则 $f(C_r)$绕原点转 n 圈. 对此仅有的解释是对某个中间的半径 r'，$f(C_{r'})$ 经过原点. 这表明对圆 $C_{r'}$ 上的某个点 α 有 $f(\alpha)=0$. 这个数 α 是 f 的一个根.

注意所有的 n 个圈都必须过原点，这与 n 次多项式有 n 个根是一致的.

我不认为这是代数，

但这并不是说代数学家不能做.

Garrett Birkhoff

练　习

第一节　域的例子

1. 设 F 是域．求出所有满足 $a=a^{-1}$ 的元素 $a\in F$.
2. 设 K 是$\mathbb{C}$ 的不包含在$\mathbb{R}$ 中的子域．证明 K 是$\mathbb{C}$ 的稠密子集.
3. 设 R 是整环，包含域 F 为其子环，且当它视为 F 上的向量空间时是有限维的．证明 R 是一个域.
4. 设 F 是恰好包含八个元素的域．证明或推翻：F 的特征为 2.

第二节　代数元与超越元

1. 设 α 是 2 的实立方根．在$\mathbb{Q}$上计算 $1+\alpha^2$ 的既约多项式.
2. 证明引理(2.7)，即$(1, \alpha, \alpha^2, \cdots, \alpha^{n-1})$是 $F[\alpha]$的基.
3. 在下列每一个域中确定 $\alpha=\sqrt{3}+\sqrt{5}$的既约多项式.

530　(a) $\mathbb{Q}$　(b) $\mathbb{Q}(\sqrt{5})$　(c) $\mathbb{Q}(\sqrt{10})$　(d) $\mathbb{Q}(\sqrt{15})$

4. 设 α 是既约多项式 x^3-3x+4 的一个复根．具体求出在 $F(\alpha)$中 $\alpha^2+\alpha+1$ 的逆，用 $a+b\alpha+c\alpha^2$，a，b，$c\in\mathbb{Q}$ 的形式表出.
5. 设 $K=F(\alpha)$，其中 α 是既约多项式 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 的根．用 α 及系数 a_i 具体表出元素 α^{-1}.
6. 设 $\beta=\zeta\sqrt[3]{2}$，其中 $\zeta=e^{2\pi i/3}$，并设 $K=\mathbb{Q}(\beta)$．证明 -1 不能写成 K 中元素的平方和.

第三节　扩域的次数

1. 设 F 是域，并设 α 是一个生成 F 的 5 次扩域的元素．证明 α^2 生成同一个扩域.
2. 设 $\zeta=e^{2\pi i/7}$，并设 $\eta=e^{2\pi i/5}$．证明 $\eta\notin\mathbb{Q}(\zeta)$.
3. 定义 $\zeta_n=e^{2\pi i/n}$．求下列元素在$\mathbb{Q}$上的既约多项式：(a)ζ_4，(b)ζ_6，(c)ζ_8，(d)ζ_9，(e)ζ_{10}，(f)ζ_{12}.
4. 设 $\zeta_n=e^{2\pi i/n}$．求下列元素在$\mathbb{Q}(\zeta_3)$上的既约多项式：(a)ζ_6，(b)ζ_9，(c)ζ_{12}.
5. 证明 F 的 1 次扩域等于 F.
6. 设 a 是正有理数，它不是$\mathbb{Q}$ 中数的平方．证明$\sqrt[4]{a}$在$\mathbb{Q}$ 上的次数为 4.
7. 确定 i 是否属于域(a)$\mathbb{Q}(\sqrt{-2})$，(b)$\mathbb{Q}(\sqrt[4]{-2})$，(c)$\mathbb{Q}(\alpha)$，其中 $\alpha^3+\alpha+1=0$.
8. 设 K 是由两个次数互素且分别为 m，n 的元素 α，β 在 F 上生成的域．证明$[K:F]=mn$.
9. 设 α，β 是$\mathbb{Q}$ 上次数为 3 的复数，并设 $K=\mathbb{Q}(\alpha, \beta)$．求$[K:\mathbb{Q}]$的可能的值.
10. 设 α，β 是复数．证明如果 $\alpha+\beta$ 和 $\alpha\beta$ 是代数数，则 α，β 也是代数的.
11. 设 α，β 是既约多项式 $f(x)$，$g(x)\in\mathbb{Q}[x]$的复根．设 $F=\mathbb{Q}[\alpha]$而 $K=\mathbb{Q}[\beta]$．证明 $f(x)$在 K 上既约当且仅当 $g(x)$在 F 上既约.
12. (a) 如果 $F\subset F'\subset K$ 是扩域．证明如果$[K:F]=[K:F']$，则 $F=F'$.
    (b) 举例说明当 F 不含于 F' 时上述结论不成立.
13. 设 $\alpha_1, \cdots, \alpha_k$ 是 F 上扩域 K 中的元素，并假设它们在 F 上都是代数的．证明 $F(\alpha_1, \cdots, \alpha_k)=F[\alpha_1, \cdots, \alpha_k]$.
14. 证明或推翻：设 α，β 是域 F 上次数分别为 d，e 的代数元．单项式 $\alpha^i\beta^j$(其中 $i=0, \cdots, d-1$，$j=0, \cdots, e-1$)构成 $F(\alpha, \beta)$在 F 上的一个基.
15. 证明或推翻：每个代数扩域是有限扩域.

第四节　直尺圆规作图

1. 用平方根表出 $\cos 15°$.

531　2. 通过(a)域论，(b)找到具体作图，证明正五边形可用直尺圆规作出.

3. 推导公式(4.12).
4. 确定正 9-边形是否能用直尺圆规作出.
5. 能否作一个正方形使其面积等于一个给定三角形的面积?
6. 设 α 是多项式 x^3+3x+1 的一个实根. 证明 α 不能用直尺圆规作出.
7. 给定 π 为超越数，证明用直尺圆规化圆为方是不可能的.(化圆为方是指作一正方形使其面积与单位半径的圆的面积是一样的.)
8. 证明“倍立方体”(也就是作出体积为 2 的正方体的边长)是不可能的.
9. (a) 参照命题(4.8)的证明，证明判别式 D 为负当且仅当两个圆不相交.
   (b) 当 $D\geqslant 0$ 及当 $D<0$ 时，从几何上确定命题(4.8)的证明中最后出现的直线.
10. 证明如果一个素数 p 具有 2^r+1 的形式，则它实际上具有 $2^{2^k}+1$ 的形式.
11. 设 C 是$\mathbb{R}$的可作实数的域. 证明 C 是$\mathbb{R}$中具有下列性质的最小子域：如果 $a\in C$ 且 $a>0$，则$\sqrt{a}\in C$.
12. 平面上的点可视为复数. 作为$\mathbb{C}$的子集，具体描述可作的点的集合.
13. 刻画在给定平面上三个点开始的情形下的可构造实数.
*14. 设三维空间中作图的规则如下：
   (a) 给定不共线的三个点. 认为它们是可以作出的.
   (b) 可以作过三个不共线的作出的点的一个平面.
   (c) 可以作以一个作出的点为圆心并过另一个作出的点的球面.
   (d) 作出的平面和球面的交点被认为是可作出的，如果它们是孤立点，即它们不是一个相交曲面的一部分.

   证明可以引入坐标并刻画可作点的坐标.

第五节 根的符号添加

1. 设 F 是特征为零的域，设 f' 表示多项式 $f\in F[x]$ 的导数，并设 g 是既约多项式且是 f 和 f' 的公因式. 证明 g^2 整除 f.
2. 对什么域 F 和什么素数 p，多项式 x^p-x 有重根?
3. 设 F 是特征为 p 的域.
   (a) 对多项式 x^p+1 应用(5.7).
   (b) 在 $F[x]$ 中把这个多项式分解成既约因式的乘积.
4. 设 α_1，…，α_n 是 n 次多项式 $f\in F[x]$ 在一个扩域 K 中的根. 求出$[F(\alpha_1,\cdots,\alpha_n):F]$的最好的上界.

532

第六节 有限域

1. 确定群$\mathbb{F}_4^+$.
2. 写出$\mathbb{F}_4$ 和$\mathbb{Z}/(4)$的加法表和乘法表，并比较它们.
3. 在域$\mathbb{F}_{13}$中求 3 的十三次根.
4. 对域$\mathbb{F}_8$ 的每个元素(6.12)确定其在域$\mathbb{F}_2$ 上的既约多项式.
5. 确定域$\mathbb{F}_3$ 上的 3 次既约多项式的个数.
6. (a) 验证(6.9)、(6.10)、(6.13)是$\mathbb{F}_2$ 上的既约因式分解.
   (b) 验证(6.11)、(6.13)是$\mathbb{Z}$上的既约因式分解.
7. 在域$\mathbb{F}_3$ 上分解 x^9-x 和 $x^{27}-x$. 证明你的分解是既约的.
8. 在(a)域$\mathbb{F}_4$ 和(b)域$\mathbb{F}_8$ 上分解多项式 $x^{16}-x$.
9. 对所有 $\alpha\in\mathbb{F}_q$ 确定使 $f(\alpha)=0$ 的$\mathbb{F}_q[x]$中所有的多项式 $f(x)$.
10. 设 K 是有限域. 证明 K 中非零元素的乘积为-1.

11. 证明$\mathbb{F}_p$的每个元素恰有一个p次根.

12. 通过证明x^q-x的两个根的差$\alpha-\beta$仍是这个多项式的根完成命题(6.19)的证明.

13. 设p是素数. 描述这样的整数n：存在一个n阶有限域K及一个元素$\alpha\in K^\times$，它在$K^\times$的阶为p.

14. 不用定理(6.4)解本题.

(a) 设$F=\mathbb{F}_p$. 求$F(x)$中二次首一既约多项式的个数.

(b) 设$f(x)$是(a)中描述的一个多项式. 证明$K=F[x]/(f)$是含有p^2个元素的域且K的元素具有$a+b\alpha$的形式，其中a，$b\in F$而α是f在K中的一个根. 证明每一个满足$b\neq 0$的这样的元素$a+b\alpha$是$F[x]$的二次既约多项式的一个根.

(c) 证明$F[x]$上的每个二次多项式在K中有一个根.

(d) 证明对一个给定的素数p，上面构造的所有域K都同构.

15. 多项式$f(x)=x^3+x+1$和$g(x)=x^3+x^2+1$在$\mathbb{F}_2$上是既约的. 设K是通过添加f的一个根得到的扩域，并设L是添加g的一个根得到的扩域. 具体地描述一个从K到L的同构.

16. (a) 在$F=\mathbb{C}$的情形中通过观察两个多项式的根证明引理(6.21).

(b) 用恒等式的不变性原理在F是任意环时推导出该结论.

第七节 函数域

1. 求三个变量的实多项式使其零点轨迹是投射出的黎曼曲面(7.9).

2. 证明U'上的连续函数的集合$\mathcal{F}(U)$构成一个环.

3. 设$f(x)$是$F[x]$中的多项式，其中F是域. 证明如果存在有理函数$r(x)$使得$r^2=f$，则r是多项式.

533

4. 参照命题(7.11)的证明，解释为什么由$g(x)\rightsquigarrow g(X)$定义的映射$F\longrightarrow\mathcal{F}(S)$是个同态.

5. 对下列多项式的黎曼曲面求分支点及黏合数据.

(a) y^2-x^2+1 (b) y^5-x (c) y^4-x-1 (d) y^3-xy-x (e) y^3-y^2-x

(f) $y^3-x(x-1)$ (g) $y^3-x(x-1)^2$ (h) y^3+xy^2+x (i) x^2y^2-xy-x

6. (a) 确定$F=\mathbb{C}[x]$上仅在点±1处分歧的三次函数域K的同构类的个数.

(b) 将对应于每个同构类的黎曼曲面的黏合数据描述为一对置换.

(c) 对每个同构类确定多项式$f(x, y)$，使得$K=F[x]/(f)$代表该同构类.

*7. 对二次扩域证明黎曼存在定理.

*8. 设S是由分支点α_1，…，α_r，曲线C_1，…，C_r及置换σ_1，…，σ_r构造的分支覆盖. 证明S连通当且仅当对称群S_n的由置换σ_ν生成的子群在指标**1**，…，$\boldsymbol{n}$上可迁地作用.

*9. 可以证明函数域的黎曼曲面S与紧有向二维流形$\overline{S}$的一个有限点集的补同胚. 这样一个曲面的亏格定义为对应的流形$\overline{S}$上洞的个数. 因而如果$\overline{S}$是球面，则S的亏格为零，而如果$\overline{S}$是环面，则S的亏格为1. 函数域的亏格定义为为其黎曼曲面的亏格. 确定由下面每个多项式定义的域的亏格.

(a) $y^2-(x^2-1)(x^2-4)$ (b) $y^2-x(x^2-1)(x^2-4)$ (c) y^3+y+x

(d) $y^3-x(x-1)$ (e) $y^3-x(x-1)^2$

第八节 超越扩域

1. 设$K=F(\alpha)$是由一个元素α生成的扩域，并设$\beta\in K$，$\beta\neq F$. 证明α在域$F(\beta)$上是代数的.

2. 证明使$\pi\rightsquigarrow e$的同构$\mathbb{Q}(\pi)\longrightarrow\mathbb{Q}(e)$是不连续的.

3. 设$F\subset K\subset L$为域. 证明$\mathrm{tr\ deg}_F L=\mathrm{tr\ deg}_F K+\mathrm{tr\ deg}_K L$.

4. 设$(\alpha_1, \cdots, \alpha_n)\subset K$是$F$上的一个代数无关集. 证明元素$\beta\in K$在$F(\alpha_1, \cdots, \alpha_n)$上超越当且仅当$(\alpha_1, \cdots, \alpha_n; \beta)$是代数无关的.

5. 证明定理(8.3).

第九节　代数闭域

1. 从定理(9.4)推导推论(9.5).
2. 证明书中作为有限域的并所构造的域 F 是代数闭域.

*3. 利用本节末的记号，对于不同的半径比较 $f(C_r)$ 的象，得出另一个有趣的几何特性：对于大的 r，曲线 $f(C_r)$ 有 n 个圈. 这可正式地表达为其整体曲率为 $2\pi n$. 对于小的 r，线性项 a_1z+a_0 支配 $f(z)$. 于是 $f(C_r)$ 构成单独一个绕 a_0 的圈. 其整体曲率仅为 2π. 当 r 变动时，圈和曲率发生了什么，请给出解释.

534

*4. 如果你能使用具有很好的图形系统的计算机，则用它来演示 $f(C_r)$ 随 r 的变化. 使用对数极坐标($\log r$, θ).

杂题

1. 设 $f(x)$ 是域 F 上的 6 次既约多项式，并设 K 是 F 上的二次扩域. 证明或推翻：f 要么在 K 上既约的，要么是两个 K 上的三次既约多项式的积.
2. (a) 设 p 是奇素数. 证明 $\mathbb{F}_p^{\times}$ 中恰好有一半元素是平方元，并且若 α, β 不是平方元，则 $\alpha\beta$ 是平方元.
   (b) 对任意奇数阶有限域证明(a).
   (c) 证明在偶数阶有限域中每个元素都是平方元.
3. 在 $\mathbb{Q}$ 上写出 $\alpha=\sqrt{2}+\sqrt{3}$ 的既约多项式并证明对每个素数 p 它是模 p 可约的.

*4. (a) 证明 $GL_2(\mathbb{Z})$ 的任意有限阶元素的阶为 1，2，3，4 或 6.
   (b) 将这个定理拓广到 $GL_3(\mathbb{Z})$ 并证明它对 $GL_4(\mathbb{Z})$ 不成立.

5. 设 c 是不等于 ± 2 的实数. 平面曲线 C：$x^2+cxy+y^2=1$ 可有理参数化. 为此，我们选择 C 上的点 $(0, 1)$ 并用过这一点的直线 L_t：$y=tx+1$ 的斜率来进行参数化. L_t 与 C 的交点可以用代数方法求得.
   (a) 具体求出这个点的方程.
   (b) 用这个过程求出方程 $x^2+cxy+y^2=1$ 在域 $F=\mathbb{F}_p$ 上的所有解，其中 c 属于这个域并且 $c\neq\pm 2$.
   (c) 证明解的个数为 $p-1$，p 或 $p+1$，并描述这个数字是如何依赖于多项式 t^2+ct+1 的.
6. 有理函数 $f(x)=p(x)/q(x)\in\mathbb{C}(x)$ 的次数定义为 p 和 q 的次数的最大值，其中 p，q 选为互素的多项式. 每个有理函数由 $x \rightsquigarrow f(x)$ 定义一个映射 $P'\longrightarrow P'$. 我们把这个映射也记为 f.
   (a) 假设 f 的次数为 d. 证明对平面上的任意点 y_0，纤维 $f^{-1}(y_0)$ 最多含有 d 个点.
   (b) 证明除了有限多个点 y_0 以外，$f^{-1}(y_0)$ 恰好由 d 个点组成. 以 f 和 $\mathrm{d}f/\mathrm{d}x$ 的形式确定有少于 d 个点的 y_0 的值.

*7. (a) 证明有理函数 $f(x)$ 生成有理函数域 $\mathbb{C}(x)$ 当且仅当它具有 $(ax+b)/(cx+d)$ 的形式，其中 $ad-bc\neq 0$.
   (b) 确定在 $\mathbb{C}$ 上为恒等的 $\mathbb{C}(x)$ 的自同构的群.

*8. 设 K/F 是有理函数域的二次扩域，设 $K=\mathbb{C}(t)$ 和 $F=\mathbb{C}(x)$. 证明存在这两个域的生成元 x'，t' 使得 $t=(\alpha t'+\beta)/(\gamma t'+\delta)$ 和 $x=(ax'+b)/(cx'+d)$，α，β，γ，δ，c，d，a，$b\in\mathbb{C}$ 满足 $t'^2=x'$.

*9. 填充下列证明概要，以给出 $K=\mathbb{C}(x)[y]/(y^2-x^3+x)$ 不是 $\mathbb{C}$ 的纯超越扩张这一事实的一个代数证明. 假设对某个 t 有 $K=\mathbb{C}(t)$. 则 x 和 y 是 t 的有理函数.

535

   (a) 必要时用 t' 代替 t，用前一个问题的结论化为 $x=(at^2+b)/(ct^2+d)$ 的情形.
   (b) 设 $y=p(t)/q(t)$. 则方程 $y^2=x(x+1)(x-1)$ 为

$$\frac{p(t)^2}{q(t)^2}=\frac{(at^2+b)((a+c)t^2+b+d)((a-c)t^2+b-d)}{(ct^2+d)^3}.$$

   要么两边的分子和分母都相等，要么在右边可以消去一个因子.
   (c) 通过分析(b)中给出的两种可能的情形完成证明.

*10. (a) 证明由模 p 约化矩阵元素所得的同态 $SL_2(\mathbb{Z})\longrightarrow SL_2(\mathbb{F}_p)$ 是个满射.
   (b) 对 SL_n 证明类似的断言.

*11. 确定 2 阶元素在 $GL_n(\mathbb{Z})$ 中的共轭类.

536

第十四章　伽罗瓦理论

总之计算是做不到的.

Evariste Galois

第一节　伽罗瓦理论的主要定理

上一章用由一个元素生成的扩域作为基本工具，我们学习了域的代数扩张．这相当于研究一个既约多项式

【1.1】
$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

的单独一个根的性质．作为本章的主题，伽罗瓦理论是这样一个多项式的所有的根及它们之间的对称的理论．

在本章中我们将把注意力限制在特征零的域上．这要理解为所有出现的域的特征是零，从现在起，我们不再具体提到这个假定．

记号 K/F 表示 K 是 F 的一个扩域．虽然这与环 R 关于理想 I 的商环的记号 R/I 有混淆的危险，但这是个传统的记号．

如我们所见到的，在由单独一个根 α 生成的域 $F(\alpha)$ 中，可以通过将它等同于形式地构造的域 $F[x]/(f)$ 来进行计算．但假定既约多项式 $f(x)$ 在扩域 K 中分解成线性因子的乘积，并且它在 K 中的根是 $\alpha_1, \cdots, \alpha_n$．我们并不清楚如何同时用这些根来进行计算．为此，需要知道这些根是如何联系起来的，而且这也依赖于特殊的情形．原则上，展开等式 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$ 就可以得到关系．这样展开后，我们知道根的和为 $-a_{n-1}$ 而其积为 $\pm a_0$，等等．然而直接解释这些关系并不是件容易的事．

537

通过许多人，特别是拉格朗日和伽罗瓦的工作，一个基本的发现是根之间的关系可以用对称的观点来理解．这个对称最早的模型是复共轭，它使实数不变而对换既约实多项式 x^2+1 的两个根 $\pm\mathrm{i}$．我们将首先观察到这样的对称存在于所有二次扩域．

一个二次扩域 K/F 是由 K 中不属于 F 的任一个元素 α 生成的．而且，α 是一个系数属于 F 的既约多项式

【1.2】
$$f(x) = x^2 + bx + c$$

的根．于是 $\alpha' = -b-\alpha$ 也是 f 的根，因而这个多项式在 K 上分解为线性因式的乘积：$f(x)=(x-\alpha)(x-\alpha')$．

α 和 α' 是同一个既约多项式的根这一事实给我们提供了对称．根据第十三章命题(2.9)，存在一个同构

【1.3】
$$\sigma: F(\alpha) \longrightarrow F(\alpha'),$$

它在 F 上是恒等映射且使得 $\alpha \rightsquigarrow \alpha'$．但两个根都生成扩域 $F(\alpha)=K=F(\alpha')$．因而 σ 是 K 的一个自同构．

自同构交换两个根 α，α'．由于 σ 在 F 上是恒等映射，它使 b 保持不变，而 $\alpha+\alpha'=b$．因

而如果$\sigma(\alpha)=\alpha'$，我们必有$\sigma(\alpha')=\alpha$. 于是得到σ^2使得$\alpha \rightsquigarrow \alpha$，而且由于$\alpha$在$F$上生成$K$，因此$\sigma^2$是恒等映射.

还要注意σ不是恒等自同构，这是因为两个根α，α'互不相等. 如果α是二次多项式(1.2)的重根，则二次公式给出$\alpha=-\frac{1}{2}b$. 这就表明$\alpha\in F$，与f是既约的假设矛盾.

由于我们假定域F是特征零的，因此二次扩域K可由添加判别式$D=b^2-4c$的一个平方根δ，也就是既约多项式x^2-D的根得到. 它的另一个根是$-\delta$，且σ交换这两个平方根.

只要K由添加一个平方根δ得到，便存在一个使$\delta \rightsquigarrow -\delta$的自同构. 例如，设$\alpha=1+\sqrt{2}$，并设$K=\mathbb{Q}(\alpha)$. 于是$\alpha$在$\mathbb{Q}$上的既约多项式为$x^2-2x-1$，而这个多项式的另一个根是$\alpha'=1-\sqrt{2}$. 存在$K$的自同构$\sigma$使得$\sqrt{2} \rightsquigarrow -\sqrt{2}$和$\alpha \rightsquigarrow \alpha'$. 重要的是要立即看到当把$K$看作是$\mathbb{R}$的子域时，这样的一个自同构不是连续的. 它是$K$的代数结构的一个对称，但它并不关心由$K$嵌入实直线所给出的几何.

由定义，扩域K的一个F-自同构是一个在子域F上为恒等映射的自同构[见第十三章(2.10)]. 换句话说，K的自同构σ是一个F-自同构，如果对所有$c\in F$，有$\sigma(c)=c$. 这样复共轭是$\mathbb{C}$上的$\mathbb{R}$-自同构，而我们刚才得到的对称σ是二次扩域K的一个F-自同构. 不难证明σ是这个扩域仅有的不是恒等映射的F-自同构. 538

K的F-自同构的群称为扩域的*伽罗瓦群*. 我们常将这个群记作$G(K/F)$. 当K/F是一个二次扩域时，伽罗瓦群$G(K/F)$是一个2阶群.

现在考虑下一个简单的例子，即双二次扩域. 我们称一个扩域K/F为*双二次的*，如果$[K:F]=4$且K由两个既约二次多项式的根生成. 每个这样的扩域都有

【1.4】
$$K = F(\alpha,\beta)$$

的形式，其中$\alpha^2=a$和$\beta^2=b$，且a和b是F的元素. 元素β生成一个中间域—F与K之间的域$F(\beta)$. 由于$K=F(\alpha,\beta)$，因此要求$[K:F]=4$意味着$F(\beta)$在F上的次数为2并且α不属于域$F(\beta)$. 因而多项式x^2-a在$F(\beta)$上既约. 类似地，多项式x^2-b在中间域$F(\alpha)$上既约.

注意K是$F(\beta)$上由α生成的次数为2的一个扩域. 我们在这个扩域上应用刚学到的关于二次扩域的东西. 用$F(\beta)$代替F，我们发现存在K的一个$F(\beta)$-自同构，它交换$x^2=a$的两个根$\pm\alpha$，把这个自同构称为σ. 由于它在$F(\beta)$上是恒等映射，σ在F上也是恒等映射，因而它也是一个F-自同构. 类似地，存在K的一个$F(\alpha)$-自同构τ，它交换x^2-b的两个根$\pm\beta$，并且τ也是一个F-自同构.

我们得到的两个自同构在根α，β上的作用如下：

【1.5】
$$\alpha \overset{\sigma}{\rightsquigarrow} -\alpha \quad \alpha \overset{\tau}{\rightsquigarrow} \alpha$$
$$\beta \overset{\sigma}{\rightsquigarrow} \beta \quad \beta \overset{\tau}{\rightsquigarrow} -\beta.$$

合成这些作用，我们看到$\sigma\tau$改变两个根α，β的符号且同构σ^2，τ^2和$\sigma\tau\sigma\tau$使α和β不变. 由于这两个根在F上生成K，因此最后这三个自同构都等于恒等映射. 因而四个自同构$\{1,\sigma,\tau,\sigma\tau\}$构成一个4阶群，满足关系

$$\sigma^2=1,\quad \tau^2=1,\quad \sigma\tau=\tau\sigma.$$

我们已经证明了伽罗瓦群 $G(K/F)$ 包含克莱因四元群. 事实上，我们马上就会看到，它等于这个群.

例如，设 $F=\mathbb{Q}$，$\alpha=\mathrm{i}$ 和 $\beta=\sqrt{2}$，于是 $K=\mathbb{Q}[\mathrm{i},\sqrt{2}]$. 这时自同构 σ 是复共轭，而 τ 保持 i 不变，使得 $\sqrt{2}\rightsquigarrow-\sqrt{2}$.

对二次或双二次扩域，次数 $[K:F]$ 等于伽罗瓦群 $G(K/F)$ 的阶. 我们给出描述这样情形发生的一般条件的两个定理，即定理(1.6)和(1.11). 这些定理将在本章后面几节证明. 539

【1.6】定理 对任意有限扩域 K/F，伽罗瓦群的阶 $|G(K/F)|$ 整除扩域的次数 $[K:F]$.

一个有限扩域 K/F 称为*伽罗瓦扩域*，如果其伽罗瓦群的阶等于其次数：

【1.7】
$$|G(K/F)|=[K:F].$$

定理(1.6)表明双二次扩域的伽罗瓦群的阶最多为 4. 因为我们已经有了四个自同构，不存在其他的自同构，因而伽罗瓦群就是克莱因四元群，这正是我们所断言的. 所有二次和双二次扩域都是伽罗瓦的.

如果 G 是域 K 的一个自同构群，则 K 中在 G 的所有自同构作用下不变的元素的集合构成一个子域，称为 G 的*不变域*. 不变域常记为 K^G：

【1.8】
$$K^G=\{\alpha\in K\mid\varphi(\alpha)=\alpha,\text{对所有 }\varphi\in G\}.$$

定理(1.6)的一个结果是当 K/F 是伽罗瓦扩域时，K 中在整个伽罗瓦群作用下不变的仅有的元素为 F 中的元素：

【1.9】推论 设 K/F 是伽罗瓦扩域，其伽罗瓦群是 $G=G(K/F)$. 则 G 的不变域为 F.

用 L 表示不变域. 则 $F\subset L$，并且这个包含表明 K 的每个 L-自同构也是一个 F-自同构，即 $G(K/L)\subset G$. 另一方面，由不变域的定义，G 的每个元素是一个 L-自同构. 因而 $G(K/L)=G$. 因为 K/F 是伽罗瓦扩域，所以 $|G|=[K:F]$，而由定理(1.6)，$|G|$ 整除 $[K:L]$. 由于 $F\subset L\subset K$，这表明 $[K:F]=[K:L]$，因而 $F=L$.

这个推论是重要的，因为它提供了一个检验伽罗瓦扩域 K 中的一个元素实际上属于 F 的办法. 我们将经常用到它.

伽罗瓦扩域对于扩域是一个很强的限制，尽管如此，仍有许多伽罗瓦扩域. 这是一个导致伽罗瓦理论的关键事实. 为了叙述描述伽罗瓦扩域的定理，我们还需要一些定义.

【1.10】定义 设 $f(x)\in F[x]$ 是一个非常数首一多项式. $f(x)$ 在 F 上的*分裂域*是 F 的一个满足下列条件的扩域 K：

(i) $f(x)$ 在 K 上分解为线性因子：$f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$，其中 $\alpha_i\in K$；

(ii) K 由 $f(x)$ 的根生成：$K=F(\alpha_1,\cdots,\alpha_n)$.

第二个条件不过是说 K 是包含所有根的 F 的最小扩域. 双二次扩域(1.4)是多项式 $f(x)=(x^2-a)(x^2-b)$ 的分裂域. 540

每个多项式 $f(x)\in F[x]$ 都有一个分裂域. 要找到一个分裂域，我们选择一个 f 在其中分裂为线性因子的扩域 L[第十三章(5.3)]，并且将 K 取为 L 的由根生成的子域 $F(\alpha_1,\cdots,\alpha_n)$.

【1.11】定理 如果 K 是多项式 $f(x)$ 在 F 上的分裂域，则 K 是 F 的伽罗瓦扩域. 反之，每个伽罗瓦扩域是某个多项式 $f(x)\in F[x]$ 的一个分裂域.

【1.12】推论 每个有限扩域包含在一个伽罗瓦扩域中.

为了从定理导出推论，设 K/F 是一个有限扩域，设 α_1，…，α_n 是 K 在 F 上的生成元，并设 $f_i(x)$ 是 α_i 在 F 上的首一既约多项式．我们将 K 扩张为积 $f=f_1\cdots f_n$ 在 K 上的分裂域 L．则 L 也是 f 在 F 上的分裂域．因而 L 是所求的伽罗瓦扩域．

【1.13】推论 设 K/F 是伽罗瓦扩域，并设 L 为中间域 $F\subset L\subset K$．则 K/L 也是伽罗瓦扩域．

因为如果 K 是多项式 $f(x)$ 在 F 上的分裂域，则它也是同一个多项式在更大的域 L 上的分裂域，因而 K 是 L 的伽罗瓦扩域．

我们回到双二次扩域．可以不用定理(1.6)证明这样的扩域的伽罗瓦群的阶为 4．所需要的全部就是下面这个初等的引理．

【1.14】命题

(a) 设 K 是 F 的一个扩域，设 $f(x)$ 是系数属于 F 的多项式，并设 σ 是 K 的一个 F-自同构．如果 α 是 $f(x)$ 在 K 中的一个根，则 $\sigma(\alpha)$ 也是一个根．

(b) 设 K 是由元素 α_1，…，α_r 生成的 F 的扩域，并设 σ 是 K 的一个 F-自同构．如果 σ 使每个生成元 α_i 都不变，则 σ 是恒等自同构．

(c) 设 K 是多项式 $f(x)$ 在 F 上的分裂域．伽罗瓦群 $G(K/F)$ 在集合 $\{\alpha_1，\cdots，\alpha_r\}$ 上忠实地作用．

证明 (a) 在上一章[第十三章(2.10)]中已得到证明．要证(b)，假定 K 由 α_1，…，α_n 生成．则 K 的每个元素都可以表为系数属于 F 的 α_1，…，α_n 的多项式[第十三章(2.6b)]．如果 σ 是一个自同构，它在 F 上是恒等映射并且保持每个元素 α_i 不变，则它保持每个系数属于 F 的 $\{\alpha_i\}$ 的多项式不变；因而它是恒等映射．第三个断言(c)由前面两个得到：第一个断言告诉我们每一个 $\sigma\in G(K/F)$ 置换集合 $\{\alpha_1，\cdots，\alpha_n\}$，而第二个断言告诉我们对这个集合的作用是忠实的． ■

541

命题(1.14)并未提到最有意思的问题：多项式的哪个根的置换扩张为分裂域的自同构？这个问题是伽罗瓦理论的中心议题．

我们将命题(1.14)应用到双二次扩域(1.4)上．在多项式 x^2-a 上应用(a)表明 K 的任意 F-自同构 φ 置换根 $\pm\alpha$．类似地，φ 置换根 $\pm\beta$．只有四个 $\{\pm\alpha，\pm\beta\}$ 的置换能这样地作用．由于元素 α，β 生成 K，(1.14b)告诉我们保持它们两个都不变的 F-自同构是恒等映射．因而我们已经找到仅有的四个自同构．这就证明了 $G(K/F)$ 是克莱因四元群．

伽罗瓦理论最重要的部分之一是中间域 L 的确定，也就是确定那些夹在 F 与 K 之间的域 $F\subset L\subset K$．伽罗瓦理论的主要定理断言当 K/F 是伽罗瓦扩域时，中间域一一地对应于伽罗瓦群的子群．这个对应的重要性不是马上就看得出来的．我们将在使用中来理解它．

对应于 $G(K/F)$ 的子群 H 的中间域是如上面所定义的 H 的不变子域 K^H．在另一个方向，如果 L 是中间域，则伽罗瓦群 $G(K/L)$ 是 $G(K/F)$ 的一个子群．这是对应于 L 的子群．

【1.15】定理 主要定理：设 K 是域 F 的伽罗瓦扩域，并设 $G=G(K/F)$ 是其伽罗瓦群．函数

$$H \rightsquigarrow K^H$$

是从 G 的子群的集合到中间域 $F\subset L\subset K$ 的集合的一一映射．其逆函数为

$$L \rightsquigarrow G(K/L).$$

这个对应具有下列性质：如果 $H=G(K/L)$，则

【1.16】 $$[K:L]=|H|, \quad 因此 \quad [L:F]=[G:H].$$

我们将在第五节证明这个定理.

域 F 和 K 也包括在中间域之中. 对应于域 F 的子群是整个群 G[见(1.9)]，而对应于 K 的群是平凡子群$\{1\}$.

我们回到双二次扩域 $K=\mathbb{Q}(\mathrm{i},\sqrt{2})$的例子，对于它 σ 是复共轭而τ交换$\sqrt{2} \rightsquigarrow -\sqrt{2}$. 其伽罗瓦群(也就是克莱因四元群)有三个真子群：

$$H_1=\{1,\sigma\}, \quad H_2=\{1,\tau\}, \quad H_3=\{1,\sigma\tau\}.$$

根据主要定理，存在三个真中间域，即这些子群的不变域 L_i. 它们都很容易确定：

542

$$L_1=\mathbb{Q}\sqrt{2}, \quad L_2=\mathbb{Q}(\mathrm{i}), \quad L_3=\mathbb{Q}(\mathrm{i}\sqrt{2}).$$

一个伽罗瓦群是有限的，因而它有有限多个子群. 但如果没有主要定理，则只有有限多个中间域这一事实并不明显. 随机地选择伽罗瓦扩域中的两个元素会生成不同的子域看起来是自然的. 但这发生的机会不大，事实上大多数元素将生成整个域 K. 双二次扩域的例子 $K=\mathbb{Q}(\mathrm{i},\sqrt{2})$就表明了这一点. 设 γ 是域 K 的任意元素. 由 γ 生成的域$\mathbb{Q}(\gamma)$必是我们找到的中间域之一. 因而如果 γ 不包含在$\mathbb{Q}(\sqrt{2})$，$\mathbb{Q}(\mathrm{i})$或$\mathbb{Q}(\mathrm{i}\sqrt{2})$中，则$\mathbb{Q}(\gamma)=K$. 这时集合$(1, \mathrm{i}, \sqrt{2}, \mathrm{i}\sqrt{2})$是 K 在 F 上的一个基，因而可以将任意元素 γ 写为如下形式：

$$\gamma=c_1+c_2\mathrm{i}+c_3\sqrt{2}+c_4\mathrm{i}\sqrt{2}, \quad 其中\ c_i\in\mathbb{Q}.$$

除非系数 c_2，c_3，c_4 中有两个为零，否则这个元素不属于三个真中间域的任何一个. 例如元素 $\mathrm{i}+\sqrt{2}$生成整个扩域 K. 在第四节我们将回到这一点.

第二节 三次方程

在上节考察了双二次扩域，我们现在转向下一类一般的例子，即三次多项式的分裂域. 三次方程

【2.1】 $$f(x)=x^3+a_2x^2+a_1x+a_0=0$$

在 16 世纪就已被数学家塔尔塔利亚(Tartalia)和卡尔达诺(Cardano)用平方根和立方根具体解出. 我们将从复习他们卓越而特别的解法开始.

当 $f(x)$的 2 次系数为零时，计算比较简单. 我们的一般方程(2.1)的平方项可以通过代换

【2.2】 $$x=x_1-a_2/3$$

消去.

我们将平方项为零的三次方程写为

【2.3】 $$f(x)=x^3+px+q,$$

其中系数 p，q 是域 F 中的元素. 方程 $f=0$ 的卡尔达诺解法由代换 $x=u-v$ 开始. 在 $f(u-v)$中合并项，得

$$f(u-v)=(u^3-v^3)-(3uv-p)(u-v)+q.$$

用变量的和代替变量 x 的要点是我们可以将方程分解开. 显然，如果两个方程

$$3uv - p = 0, \quad u^3 - v^3 + q = 0$$

成立，则有 $f(u-v)=0$. 而由于有两个变量，我们希望得到这样一对方程的解，尽管在之前不清楚这是否有用. 解第一个方程，得 $v=p/3u$ 并代入第二个方程. 去分母后得到 543

$$3^3u^6 - p^3 + 3^3u^3q = 0.$$

奇迹般地把这个方程化为 u^3 的二次方程. 令 $y=u^3$，它化为

【2.4】
$$3^3y^2 + 3^3qy - p^3 = 0.$$

这个方程可用二次公式求解：

【2.5】
$$y = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

这样得到卡尔达诺公式 $x=u-v$，其中

【2.6】
$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}, \quad v = \sqrt[3]{u^3+q} = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

后面将可以不用具体计算而证明这个一般形式的解存在[见(7.6)].

现在查看一个既约三次多项式 $f(x)$ 的伽罗瓦理论. 可以假设 $f(x)$ 具有(2.3)的形式. 设 K 是 $f(x)$ 在 F 上的分裂域，并设 α_1，α_2，α_3 是 $f(x)$ 在 K 中的根，它们为任意排序，因而

【2.7】
$$f(x) = x^3 + px + q = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3).$$

展开等式的右边，我们得到关系

【2.8】
$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$
$$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 = p$$
$$\alpha_1\alpha_2\alpha_3 = -q.$$

第一个关系表明第三个根 α_3 属于由前两个根生成的域. 这样我们有域链

$$F \subset F(\alpha_1) \subset K,$$

并设 $K=F(\alpha_1, \alpha_2)=F(\alpha_1, \alpha_2, \alpha_3)$. 我们用 L 表示 $F(\alpha_1)$. 这就出现两种基本上不同的情形，即要么

【2.9】
$$L = K \text{ 要么 } L < K.$$

用根来描述，当后两个根 α_2 和 α_3 可以用 α_1 和 F 中的元素表出时，也就是如果它们可以写成系数属于 F 的 α_1 的多项式的时候，第一种情形发生[见第十三章(2.6)]. 当后两个根不能以这样的方式表出时第二种情形发生.

例如，设 $f(x)=x^3-2$. 这个多项式的三个根是 $\alpha_1=\sqrt[3]{2}$，$\alpha_2=\zeta\sqrt[3]{2}$，$\alpha_3=\zeta^2\sqrt[3]{2}$，其中$\sqrt[3]{2}$表示 2 的实立方根而 $\zeta=e^{2\pi i/3}$. 由于 α_1 是实数，域$\mathbb{Q}(\alpha_1)$包含在$\mathbb{R}$中. 其他两个根是复的，不能包含在其中. 因此如果 $F=\mathbb{Q}$ 且 $L=\mathbb{Q}(\alpha_1)$，我们就得到第二种情形. 另一方面，如果令 $F=\mathbb{Q}(\zeta)$，则 $F(\alpha_1)$包含 α_2，因而得到第一种情形. 544

为了分析(2.9)的两种情形，我们考虑既约多项式 $f(x)$ 在域 L 中分解的方法. 由假设，$f(x)$在 $F[x]$中是既约的，且它在 $K[x]$中分解为线性因式的乘积. 在环 $L[x]$中，$f(x)$有因式 $(x-\alpha_1)$：

【2.10】
$$f(x)=(x-\alpha_1)h(x),$$
其中 $h(x)$ 是系数属于 L 的二次多项式．在更大的域 K 中用 $x-\alpha_1$ 除也得到同样的结果．对比(2.7)，我们看到在 $K[x]$ 中 $h(x)=(x-\alpha_2)(x-\alpha_3)$．因而 $L<K$ 当且仅当 $h(x)$ 在 L 上既约．在这种情形，$L(\alpha_2)$ 在 L 上的次数为 2．而且由于我们假定 $f(x)$ 在 F 上既约，在两种情形都有 $[L:F]=3$．因而有

【2.11】
$$[K:F]=\begin{cases}3 & \text{如果 } L=K\\ 6 & \text{如果 } L<K.\end{cases}$$

【2.12】例　多项式 $f(x)=x^3+3x+1$ 在 $\mathbb{Q}$ 上是既约的，且它仅有一个实根．要看到只有一个实根，我们注意到 f 的导数在实直线上不为零．因而 $f(x)$ 定义了实变量 x 的一个递增函数．它只取一次 0 值．分裂域 K 里面还包含两个复根，实根不会生成它．因而在这种情形有 $[K:\mathbb{Q}]=6$.

另一方面，多项式 $f(x)=x^3-3x+1$ 在 $\mathbb{Q}$ 上的分裂域的次数为 3．它的一个根是 $\eta_1=2\cos 2\pi/9=\zeta+\zeta^8$，其中 $\zeta=e^{2\pi i/9}$．用多项式可直接验证这一点．但实际上，我们是通过计算 η_1 在 $\mathbb{Q}$ 上的既约多项式得到这个例子的．计算这个多项式的办法是猜出它的根．注意到 η_1 是 1 的九次方根与其逆的和．还有另外两个这类的和：$\eta_2=\zeta^2+\zeta^7$ 和 $\eta_3=\zeta^4+\zeta^5$．我们猜测这些是其他的根并展开 $(x-\eta_1)(x-\eta_2)(x-\eta_3)$，得到 f．本例中 η_2 碰巧等于 η_1^2-2 而 $\eta_3=-\eta_1-\eta_2$．因而 $K=F(\eta_1)$.

我们回到一个一般的三次方程．根据定理(1.11)，伽罗瓦群 $G=G(K/F)$ 的阶是扩域的次数 $[K:F]$．对三次方程，这个次数完全确定了群 G．命题(1.14)告诉我们 G 忠实地作用在根的集合 $(\alpha_1, \alpha_2, \alpha_3)$ 上．这些根是互不相同的[第十三章(5.8)]．因而 G 是阶为 6 的对称群 S_3 的子群．如果 $[K:F]=6$，则 G 是整个对称群．在这种情形，根的任意置换由 K 的一个 F-自同构实现．另一方面，S_3 仅有的 3 阶子群是交错群 A_3，它是一个循环群．因而如果 $[K:F]=3$，则 $G=A_3$．在这种情形只有循环置换和恒等映射能拓广为 F-自同构．这样一个三次既约多项式的根或有二面体对称或有循环对称．但这些对称是代数的；当将 K 视为复平面上的点集时它们将不是 K 的对称．

545

我们在次数 $[K:F]$ 为 6 的情形确定中间域．(当 $[K:F]=3$ 时没有真正介于 F 与 K 之间的中间域．)对称群 S_3 有三个 2 阶的共轭子群和一个 3 阶子群 A_3．有三个明显的中间域：$F(\alpha_1)$，$F(\alpha_2)$，$F(\alpha_3)$．它们是 K 中同构但不相等的子域，并且它们对应于三个 2 阶子群．但对应于子群 A_3 的子域并不明显．我们将这个神秘的子域记为 L．根据主要定理，$G(K/L)=A_3$．因此 $[K:L]=3$ 且 $[L:F]=2$．因而 L 是 F 的二次扩域，它可通过添加一个平方根得到．主要定理已经告诉我们一个有趣的事实：K 中包含 F 中一个元素的平方根 δ．并且由于只有一个二次的中间扩域，这个平方根在本质上是唯一的．主要定理还告诉我们 L 是子群 A_3 的不变域．因而根的偶置换使 δ 不变，而奇置换不能使之不变．要求的元素是

【2.13】
$$\delta=(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3).$$
根的置换使 δ 乘上一个置换的符号．因此 δ 不被 $G(K/F)=S_3$ 的所有元素保持不变，于是 $\delta\notin F$．但 δ^2 在每一个置换作用下不变．推论(1.9)告诉我们 $\delta^2\in F$.

对任意三次多项式 $f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$，元素

【2.14】
$$D=(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$$
称为多项式的判别式．它是域 F 中的元素且它为零当且仅当 $f(x)$ 的两个根相等．因此它类似于二次多项式 $x^2+bx+c=(x-\alpha_1)(x-\alpha_2)$ 的判别式 $b^2-4c=(\alpha_1-\alpha_2)^2$．如果三次多项式 f 既约，则其根互不相同，因而 $D\neq 0$．

三次多项式的判别式是 F 中的元素这一事实由推论(1.9)得到，但并不是平凡的．我们将在下节抽象地加以证明，但它也可以通过直接计算验证．利用公式(2.8)，可用系数 p，q 来计算判别式．即

【2.15】
$$D=-4p^3-27q^2.$$

【2.16】命题 *三次既约多项式 $f(x)\in F[x]$ 的判别式是 F 中元素的平方当且仅当分裂域的次数为 3.*

如果我们随机地选择一个整系数多项式，则判别式不是$\mathbb{Q}$中元素的平方的机会很大．例如 x^3+3x+1 的判别式是 -135．另一方面，x^3-3x+1 的判别式是 81，这是个平方数．这与 $[K:F]=3$这一事实相符[见(2.12)]．

命题的证明 如果 D 不是平方数，则 $\delta\notin F$，因而$[F(\delta):F]=2$．由于 $\delta\in K$，$[K:F]$被 2 整除，因而由(2.11)有$[K:F]=6$．另一方面，如果 $\delta\in F$，则伽罗瓦群 $G=G(K/F)$的每个元素保持 δ 不变．由于奇置换改变 δ 的符号，因而它们不属于 G，因此 $G\neq S_3$．因而$[K:F]=3$． ■

546

这样一个命题怎么会是对的呢？一定有一个用 α_1，δ 以及系数 p，q 表出第二个根 α_2 的公式．这个公式存在，并且其具体计算是很有启发性的．

第三节 对称函数

伽罗瓦理论与确定能拓广为域的自同构的那些多项式的根的置换问题有关．本节中我们看一下每个置换都能拓广的简单情形，即当根是无关变量时的情形．

设 R 是任意环，考虑 n 个变量 u_i 的多项式环 $R[u_1,\cdots,u_n]$．通过置换变量，可使$\{1,\cdots,n\}$的一个置换 σ 在多项式上作用．这里必须确定置换如何作用．我们保持自同构从左边作用．则 σ 的作用通过对下标的逆置换实现：

【3.1】
$$f=f(u_1,\cdots,u_n)\overset{\sigma}{\rightsquigarrow} f(u_{1\sigma^{-1}},\cdots,u_{n\sigma^{-1}})=\sigma f.$$
显然这是 $R[u]$的一个自同构．由于它在 R 上的作用是恒等映射，σ 称为一个 R-自同构．因而对称群 S_n 通过R-自同构在多项式环$R[u]$上作用．一个多项式称为*对称的*，如果它在所有的置换作用下不变．

对称多项式是容易描述的．为了使 g 是对称的，如 $u_1^2u_2$ 和 $u_2^2u_3$ 这样仅相差下标的置换的两个$\{u_1,\cdots,u_n\}$的单项式在 g 中必须有相同的系数．一个包含给定的单项式的对称多项式必包含整个轨道．这样
$$g(u)=(u_1^3+u_2^3+u_3^3)+5(u_1^2u_2+u_1^2u_3+u_2^2u_3+u_2^2u_1+u_3^2u_2+u_3^2u_1)-u_1u_2u_3$$
是一个三个变量的三次对称多项式．

有 n 个特殊的整系数对称多项式，称为*初等对称函数* s_i．

【3.2】
$$s_1=u_1+u_2+\cdots+u_n$$
$$s_2=u_1u_2+u_1u_3+\cdots+u_{n-1}u_n=\sum_{i<j}u_iu_j$$

$$s_3 = \sum_{i<j<k} u_i u_j u_k$$

$$\vdots$$

547

$$s_n = u_1 u_2 \cdots u_n.$$

它们是$(x-u_1)(x-u_2)\cdots(x-u_n)$作为$x$的多项式展开式的系数：

【3.3】 $$p(x)=(x-u_1)(x-u_2)\cdots(x-u_n)=x^n-s_1x^{n-1}+s_2x^{n-2}-\cdots\pm s_n.$$

这里我们反转下标的顺序并且交错各项的符号．因为$p(x)$关于下标的置换是对称的，所以系数s_i都是对称的．

对称函数的主要定理断言初等对称函数生成所有对称多项式的环．

【3.4】定理　*每个对称多项式$g(u_1, \cdots, u_n)\in R[u]$可以用唯一的方式写成初等对称函数$s_1, \cdots, s_n$的多项式．换言之，设$z_1, \cdots, z_n$为变量．对每个对称多项式$g(u)$，存在唯一的多项式$\varphi(z_1, \cdots, z_n)\in R[z_1, \cdots, z_n]$，使得*

$$g(u_1,\cdots,u_n)=\varphi(s_1,\cdots,s_n).$$

这个定理的证明见本节末．

例如

【3.5】 $$u_1^2+\cdots+u_n^2=s_1^2-2s_2.$$

多项式$p(x)$(3.3)的判别式定义为

【3.6】 $$D=(u_1-u_2)^2(u_1-u_3)^2\cdots(u_{n-1}-u_n)^2 = \prod_{i<j}(u_i-u_j)^2=\pm\prod_{i\neq j}(u_i-u_j),$$

它也许是最重要的对称多项式．判别式的最后两个表达式在有的时候用起来是很方便的，但遗憾的是它们会相差一个符号．从D的第二个表达式到最后一个需要改变$\frac{1}{2}n(n-1)$次符号，因而代替记号$\pm$的正确的符号是

【3.7】 $$(-1)^{n(n-1)/2}.$$

显然D是一个整系数对称多项式．因而定理(3.4)告诉我们它可以写成一个初等对称函数的整多项式．换言之，存在一个多项式

【3.8】 $$\Delta(z_1,\cdots,z_n)\in \mathbb{Z}[z_1,\cdots,z_n]$$

使$D=\Delta(s_1, \cdots, s_n)$．遗憾的是，$D$的初等对称函数的表达式是非常复杂的．对$n>3$我不知道它是什么．

对$n=2$容易计算判别式：

548

【3.9】 $$(u_1-u_2)^2=s_1^2-4s_2.$$

这是所熟悉的二次多项式$p(x)=x^2-s_1x+s_2$的判别式的公式．当$n=3$时，判别式的公式就已经太复杂而难于记住：

【3.10】 $$(u_1-u_2)^2(u_1-u_3)^2(u_2-u_3)^2=s_1^2s_2^2-4s_2^3-4s_1^3s_3-27s_3^2+18s_1s_2s_3.$$

重要的是注意这样一个表达式是$\mathbb{Z}[u_1, \cdots, u_n]$的一个恒等式．当对变量$u_i$作了代入之后它仍成立．如果给定环$R$中的特定元素$\{\alpha_1, \cdots, \alpha_n\}$，则可以用$\alpha_i$代替$p(x)$中的$u_i$展开所得

到的多项式：

$$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)=x^n-b_1x^{n-1}+b_2x^{n-2}-\cdots\pm b_n.$$

调整下标和符号，使之与(3.3)一致．于是

$$b_i=s_i(\alpha_1,\cdots,\alpha_n),$$

且

$$\prod_{i<j}(\alpha_i-\alpha_j)^2=\Delta(b_1,\cdots,b_n).$$

这由用 α_i 替代 u_i 得到．

同样重要的是对称多项式用初等对称函数表示的表达式也是唯一的．

【3.11】推论 *在初等对称函数 s_1，…，s_n 之间不存在多项式关系．等价地，$R[u]$ 由 $\{s_i\}$ 生成的子环 $R[s_1,\cdots,s_n]$ 同构于 n 个变量的多项式环 $R[z_1,\cdots,z_n]$.*

这是定理(3.4)中唯一性的复述．

下面是一个应用推论的范例：设

【3.12】
$$f(x)=x^n-a_1x^{n-1}+a_2x^{n-2}-\cdots\pm a_n$$

是一个系数属于环 R 的多项式．我们定义 $f(x)$ 的判别式为 R 的元素 $\Delta(a_1,\cdots,a_n)$，其中 $\Delta(z_1,\cdots,z_n)$ 是多项式(3.8)．由于这个多项式是唯一的，无论多项式是否是 $R[x]$ 中线性因子的乘积，判别式都是有定义的．

例如，设 $n=3$．则公式(3.10)表明

【3.13】
$$\Delta(0,p,-q)=-4p^3-27q^2,$$

这与三次多项式 x^3+px+q 的判别式的公式(2.15)是一致的．

可以用待定系数法来计算对称多项式的初等对称函数表达式．为了应用这个方法，我们注意到初等对称函数 s_i 在变量 u 上的次数为 i．这是为什么选择 i 为其下标的原因．因而我们为变量 z_i 指定一个权 i，并定义单项式 $z_1^{e_1}z_2^{e_2}\cdots z_n^{e_n}$ 的带权次数为

【3.14】
$$e_1+2e_2+\cdots+ne_n.$$

在 z 的带权次数为 d 的多项式中用 s_i 代替 z_i 产生一个 u_1，…，u_n 的(普通)次数为 d 的多项式．

例如，要用初等对称函数计算三次多项式的判别式，我们注意到它关于 u 的次数为 6．有七个带权次数为 6 的 z_1，z_2，z_3 的单项式：

【3.15】
$$z_1^6,z_1^4z_2,z_1^3z_3,z_1^2z_2^2,z_1z_2z_3,z_2^3,z_3^2.$$

因而 D 是这些单项式的线性组合．要计算其系数，我们求 D 在一些特殊的多项式上的取值：令 $f(x)=x^2(x-1)$，可得 $D=0$，$s_1=1$，$s_2=s_3=0$．由于(3.15)中仅有的不涉及 z_2 和 z_3 的单项式是 $z_1{}^6$，因此在判别式中 $z_1{}^6$ 的系数为零．例如，可以用特殊的多项式 x^3-x 和 x^3-1 计算 $z_2{}^3$ 和 $z_3{}^2$ 的系数．

定理(3.4)的证明 作为例子，先做出对称多项式

$$f(x)=u_1^2u_2+u_1^2u_3+u_2^2u_1+u_2^2u_3+u_3^2u_1+u_3^2u_2$$

的情形来热一下身．为分析它，第一步是取 $u_3=0$．我们得到剩下的两个变量 u_1，u_2 的对称多

549

项式 $f^0=u_1^2u_2+u_2^2u_1$. 用 $s_1^0=u_1+u_2$ 和 $s_2^0=u_1u_2$ 表示 u_1, u_2 的初等对称函数. 我们注意到 $f^0=s_1^0s_2^0$.

第二步是比较 f 与三个变量的多项式 s_1s_2. 计算多项式 $f-s_1s_2$, 其中 $s_1=u_1+u_2+u_3$ 而 $s_2=u_1u_2+u_1u_3+u_2u_3$, 会发现 $f-s_1s_2=-3u_1u_1u_3$. 我们看到这个多项式是 $-3s_3$. 因而 $f=s_1s_2-3s_3$.

一般情形是类似的. 当 $n=1$ 时没有什么要证的, 因为这时 $u_1=s_1$. 进行归纳, 假设定理对 $n-1$ 个变量的情形已证明. 给定 u_1, …, u_n 的一个对称多项式 f, 考虑用零代入最后一个变量得到的多项式 f^0: $f^0(u_1, \cdots, u_{n-1})=f(u_1, \cdots, u_{n-1}, 0)$. 我们注意到 f^0 是 u_1, …, u_{n-1}的对称多项式. 由归纳假设, f^0 可以表为$\{u_1, \cdots, u_{n-1}\}$的初等对称函数的多项式, 我们将这些初等对称函数记为

$$s_1^0=u_1+\cdots+u_{n-1},\cdots,s_{n-1}{}^0=u_1\cdots u_{n-1}.$$

于是可以记 $f^0=g(s_1^0, \cdots, s_{n-1}^0)$. 而且, 由多项式 s_i 的定义,

550

$$s_i^0=s_i(u_1,\cdots,u_{n-1},0),\quad 如果\ i=1,\cdots,n-1.$$

考虑多项式

$$p(u_1,\cdots,u_n)=f(u_1,\cdots,u_n)-g(s_1,\cdots,s_{n-1}),$$

它为 u_1, …, u_n 的多项式. 作为对称多项式的差, 这个多项式是对称的. 它还具有性质 $p(u_1, \cdots, u_{n-1}, 0)=0$. 因而在 p 中出现的每一个单项式被 u_n 整除. 由对称性, 对每个 i 来讲, p 可以被 u_i 整除, 因而能被 s_n 整除. 因此有对称多项式 h 使得

【3.16】 $$f(u_1,\cdots,u_n)=g(s_1,\cdots,s_{n-1})+s_nh(u_1,\cdots,u_n).$$

现在考虑 $h(u_1, \cdots, u_n)$. 对次数作归纳, 可得 h 是对称函数的多项式, 因此 f 也是.

剩下的是 $\varphi(s_1, \cdots, s_n)$ 的唯一性的证明. 唯一性是指只存在一个变量 z_i 的多项式 $\varphi(z_1, \cdots, z_n)$使得作为 u_1, …, u_n 的多项式 $\varphi(s_1, \cdots, s_n)=f(u_1, \cdots, u_n)$. 换言之, 使 $z_i \rightsquigarrow s_1$的代入映射

$$\sigma: R[z]\longrightarrow R[u]$$

的核为零. 为证这一点, 假定对某个 $\varphi\in R[z]$, 有 $\varphi(s_1, \cdots, s_n)=0$. 在这个表达式中取 $u_n=0$, 我们仍然得零: $\varphi(s_1^0, \cdots, s_{n-1}^0, 0)=0$. 对 n 作归纳, 这蕴涵 $\varphi(z_1, \cdots, z_{n-1}, 0)=0$. 因而 z_n 整除 $\varphi(z)$, 我们可记 $\varphi(z)=z_n\psi(z)$. 于是 $0=\varphi(s)=s_n\psi(s)=u_1\cdots u_n\psi(s)$. 由于在多项式环 $R[u]$中积 $u_1\cdots u_n$ 不是零因子, 因此 $\psi(s)=0$. 多项式 $\psi(z)$关于 z 的总次数小于 $\varphi(z)$的总次数, 因而可对总次数应用归纳法得到 $\psi=0$. 因此也有 $\varphi=0$. ■

现在假设 $R=F$ 是一个域. 则也可以考虑变量 u_i 的有理函数域, 即 $F[u_1, \cdots, u_n]$的分式域. 对称群也在这个域上作用, 而且相应的断言也成立:

【3.17】定理 *每个对称有理函数是 s_1, …, s_n 的有理函数.*

证明 设 $r(u)=f(u)/g(u)$是一个对称有理函数, 其中 f, $g\in F[u]$. 我们可以通过将所有 σg 乘起来构造一个对称函数:

$$G=\prod_{\sigma\in S_n}\sigma g$$

是一个对称多项式. 于是 $G(u)r(u)$是一个对称有理函数, 它也是$\{u_1, \cdots, u_n\}$的多项式——对

称多项式．由定理(3.4)，$G(u)$和$G(u)r(u)$都是初等对称函数$\{s_i\}$的多项式．这样$r(u)$是$\{s_i\}$的有理函数．■

下面这一对域

【3.18】 $$F(s)=F(s_1,\cdots,s_n)\subset F(u_1,\cdots,u_n)=F(u)$$

551

是伽罗瓦扩域的例子．这由定理(1.11)得到，这是因为$F(u)$是多项式$p(x)$的分裂域(3.3)且u_1，…，u_n互不相同．由命题(1.14)，伽罗瓦群$G=G(F(u)/F(s))$在根上忠实地作用．另一方面，由构造可知G包含整个对称群．因而$G=S_n$．作为推论，我们得到$[F(u):F(s)]=n!$．不必说，这是可以直接证明的．

第四节 本 原 元

在第一节的结尾，我们看到双二次扩域K/F中一个一般性选择的元素生成K．这一类型的一般性断言可以作为伽罗瓦理论主要定理的推论导出．但我们将反过来，先直接证明它，然后在主要定理的证明中应用这一事实．

【4.1】定理 *本原元的存在性：设K是特征为零的域F的有限扩域．则存在一个元素$\gamma\in K$使得$K=F(\gamma)$．*

一个生成扩域K/F的元素γ称为K在F上的本原元．因而定理可以复述为域F的每个有限扩域有一个本原元．我们在这里重复域F的特征为零这个一般性的假定，是因为对于特征p的域这个定理并不成立．

定理(4.1)的证明 我们对K的生成元的个数用数学归纳法证明．设$K=F(\alpha_1,\cdots,\alpha_n)$．如果$n=1$,没有什么可证的．对$n>1$，归纳原理允许我们假设定理对中间域$K_1=F(\alpha_1,\cdots,\alpha_{n-1})$成立．因而可以假设$K_1$由单独一个元素$\beta$生成．于是$K=K_1(\alpha_n)=F(\beta,\alpha_n)$．我们必须证明这个域中有一个本原元．因此化为$n=2$的情形，这样$K$由两个元素$\alpha$，$\beta$生成．

设$f(x)$，$g(x)$是α，β在F上的既约多项式，并设K'是使得f和g完全分裂的K的扩域[第十三章(5.3)]．将它们的根记作$\alpha=\alpha_1$，…，α_m和$\beta=\beta_1$，…，β_n．由第十三章(5.8)，元素α_i是互不相同的．

我们要证对大多数$c\in F$，线性组合$\gamma=\beta+c\alpha$生成K．用L记域$F(\gamma)$．只要证$\alpha\in L$即可，因为如果这样，则$\beta=\gamma-c\alpha$也将属于L，且这表明$L=K$．我们证明α属于L的方法是间接的：确定它在L上的既约多项式．我们知道这是$L[x]$中以α为根的次数最低的首一多项式．

从$f(x)$的一个根α开始．诀窍是用多项式$g(x)$作出另一个以α为根的多项式，即$h(x)=g(\gamma-cx)$．注意$h(x)$的系数属于L且$h(\alpha)=0$．如果证明了f和h在$L[x]$中的最大公因式为$x-\alpha$，则得到$x-\alpha$的系数之一$-\alpha\in L$．现在无论在$L[x]$或$K'[x]$中f和h的首一最大公因式都是相同的[第十三章(5.4)]．因而我们可以在$K'[x]$中作计算．在这个环中f是线性因式$x-\alpha_i$的乘积，只需证明它们都不整除h，也就是除去$\alpha=\alpha_1$外，元素α_i中没有一个是$h(x)$的根．至此，剩下的就是计算h的根．

552

由于g的根为β_j，$h(x)=g(\gamma-cx)$的根由解关于x的方程

$$\gamma-cx=\beta_j$$

得到．由于$\gamma=\beta+c\alpha$，因此根为$(\gamma-\beta_j)/c=(\beta-\beta_j)/c+\alpha$．我们希望这些根不同于$\alpha_i$，$i\neq 1$．只要$c$不取有限多个值

【4.2】
$$-\frac{\beta_j-\beta}{\alpha_i-\alpha},$$

(其中i，$j\neq 1$，1)这就可以了． ■

【4.3】例 考虑域$K=\mathbb{Q}[\mathrm{i},\sqrt[3]{2}]$．这个域在$\mathbb{Q}$上的次数为6[见第十三章(3.5d)]．用前面证明中的记号，我们有$\beta_1=\mathrm{i}$，$\beta_2=-\mathrm{i}$，以及$\alpha_1=\sqrt[3]{2}$，$\alpha_2=\zeta\sqrt[3]{2}$，$\alpha_3=\zeta^2\sqrt[3]{2}$，其中$\zeta=e^{2\pi i/3}$．条件(4.2)成为

$$\sqrt[3]{2}c\neq\frac{\pm\mathrm{i}-\mathrm{i}}{\zeta^v-\zeta},\quad v=1,2.$$

除了$c=0$外，这个条件对所有$c\in\mathbb{Q}$成立．因而对每个有理数$c\neq 0$，$\gamma=\mathrm{i}+c\sqrt[3]{2}$在$\mathbb{Q}$上生成$K$．当然，两个元素$\beta$，$\alpha$的许多其他的组合也将生成$F(\beta,\alpha)$．在这个例子中乘积$\mathrm{i}\sqrt[3]{2}$也生成$K$．

由于两个原因，定理(4.1)很重要．首先，如果知道了γ在F上的既约多项式，那么在形如$F(\gamma)$的扩域中的具体计算是容易的．其次，由于有限扩域具有$F(\gamma)$的形式，可以由关于代数元的事实导出它们的性质．正是这一点对我们最为重要．

定理(4.1)的威力通过将它应用于域的自同构的研究而显现出来．考虑有限群G在域K上的作用，将其不变域K^G记作F．

【4.4】命题 设G是域K的有限自同构群，设F是其不变域．设$\{\beta_1,\cdots,\beta_r\}$是一个元素$\beta=\beta_1\in K$在$G$的作用下的轨道．则$\beta$在$F$上是代数的，它在$F$上的次数为$r$，且它在$F$上的既约多项式是$g(x)=(x-\beta_1)\cdots(x-\beta_r)$．

553

注意作为轨道的阶，β的次数整除群的阶．

证明 设$f(x)$是β在F上的既约多项式．由于$f(x)$在G的作用下不变，每个元素β_i是f的一个根(1.14)，因而g整除f．而且g在$\{\beta_1,\cdots,\beta_r\}$的所有置换下不变，因此在$G$的作用下不变，这个作用置换轨道．因而$g(x)\in F[x]$．由于$f$既约，所以$g=f$． ■

这个命题提供了一种确定F上的伽罗瓦扩域K中一个元素β的既约多项式的一种方法．例如，设K为双二次扩域$\mathbb{Q}[\mathrm{i},\sqrt{2}]$，并设$\beta=\mathrm{i}+\sqrt{2}$．$K/\mathbb{Q}$的伽罗瓦群是克莱因四元群，$\beta$的轨道由四个元素$\pm\mathrm{i}\pm\sqrt{2}$组成．因而$\beta$在$\mathbb{Q}$上的既约多项式为

$$\begin{aligned}&(x-\mathrm{i}-\sqrt{2})(x-\mathrm{i}+\sqrt{2})(x+\mathrm{i}-\sqrt{2})(x+\mathrm{i}+\sqrt{2})\\&\quad=(x^2-2\mathrm{i}x-3)(x^2+2\mathrm{i}x-3)=x^4-2x^2+9.\end{aligned}$$

也可通过计算β的幂并找出它们之间最低次的线性关系确定这个多项式(见第十三章第三节)．然而，我们更喜欢用这个方法是因为它总是得到既约多项式．

【4.5】推论 设K/F是伽罗瓦扩域，并设$g(x)$是$F[x]$中的既约多项式．如果g在K中有一个根，则它在$K[x]$中分解成线性因式的乘积．

证明 根据推论(1.9)，F是伽罗瓦群$G=G(K/F)$的不变域．设β是$g(x)$在K中的一个根．由命题(4.4)，β在F上的既约多项式是$(x-\beta_1)\cdots(x-\beta_r)$，其中$\{\beta_1,\cdots,\beta_r\}$是$\beta$的$G$-轨

道. 由于$g(x)$是β的既约多项式，它等于这个积，因而它在K上分解成线性因式的乘积，这正是所断言的. ■

推论特别告诉我们每个伽罗瓦扩域是一个分裂域，这是定理(1.11)的一部分. 因为取K在F上的任意生成元α，β，…，并设$f(x)$是它们的既约多项式的乘积. 则f在K中完全分裂，因此K是f的分裂域.

【4.6】定理 设G是域K的一个n阶自同构群，设F是其不变域. 则有$[K:F]=n$.

证明 命题(4.4)表明K的每个元素β在F上是代数的且其次数整除$n=|G|$. 本原元定理表明整个扩域K/F的次数也以n为界. 为此，我们如下构造一个扩域链：选择一个K中不属于F的元素α_1，令$F_1=F(\alpha_1)$. 则$[F_1:F]\leqslant n$. 如果$F_1\neq K$，选择一个不属于F_1的元素$\alpha_2\in K$,并令$F_2=F(\alpha_1, \alpha_2)$. 由本原元定理，$F_2$由单独一个元素$\gamma$生成，且由第十三章推论(3.6)，$\gamma$在$F$上的次数以$n$为界. 因而$[F_2:F]\leqslant n$. 这样继续下去，我们得到一个链$F<F_1<F_2\cdots$,其中对所有$i$有$[F_i:F]\leqslant n$. 这必为一个有限链. 因而对某个$i$有$F_i=K$，并且$[K:F]\leqslant n$.

554

再次用定理(4.1)，我们得到K有一个本原元β：$K=F(\beta)$. G中使β不变的任意元在$K=F(\beta)$上的作用是恒等映射. 由于假定了G是K的自同构群，因此恒等元素是仅有的这样的元. 因而β的稳定子是$\{1\}$，从而轨道的阶为n. 由命题(4.4)，β在F上的次数为n，因而$[K:F]=n$. ■

运用我们刚证明的定理，可以导出在第一节叙述的第一个定理，即定理(1.6). 这个定理指出，对任意有限扩域K/F，其伽罗瓦群的阶整除其次数. 为证明这一点，令$G=G(K/F)$. 则G在K上作用，因而由定理(4.6)，$|G|=[K:K^G]$. 且由于$F\subset K^G\subset K$，$[K:K^G]$整除$[K:F]$.

定理(4.6)也为我们提供了推论(1.9)的一个逆：

【4.7】推论 设G是域K的有限自同构群，并设F是其不变域. 则K是F的伽罗瓦扩域，且其伽罗瓦群是G.

证明 由不变域的定义，G的元素是K的F-自同构. 因此$G\subset G(K/F)$. 由于$|G(K/F)|\leqslant[K:F]$且$[K:F]=|G|$，由此得$|G(K/F)|=[K:F]$，因而$G=G(K/F)$. ■

我们可以得到一些有趣的例子，并通过考虑y的有理函数域$\mathbb{C}(y)=K$的自同构来说明命题(4.4)和定理(4.6). 例如，设σ，τ是由$y \rightsquigarrow -y$和$y \rightsquigarrow \mathrm{i}y^{-1}$定义的$K$的自同构. 自同构$\{1, \sigma, \tau, \sigma\tau\}$构成一个4阶群$G$.

【4.8】命题 设K和G如上. 不变域$F=K^G$是$w=y^2-y^{-2}$的有理函数域$\mathbb{C}(w)$.

换言之，每一个在σ下不变的有理函数$f(y)$可以写为w的一个有理函数.

证明 首先，G的确使$w=y^2-y^{-2}$不变，所以w属于不变域. 因而不变域F包含域$\mathbb{C}(w)$. 其次，我们计算y在F上的既约多项式. y的轨道为$\{y, \mathrm{i}y^{-1}, -y, -\mathrm{i}y^{-1}\}$，因而命题(4.4)告诉我们$y$的既约多项式是$(x-y)(x-\mathrm{i}y^{-1})(x+y)(x+\mathrm{i}y^{-1})=x^4-wx^2-1$. 这个多项式的系数属于$\mathbb{C}(w)$,因而$y$在这个域上的次数为4. 由此得$[K:\mathbb{C}(w)]=4$. 另一方面，$\mathbb{C}(w)\subset F\subset K$，且由于$|G|=4$,定理(4.6)告诉我们$[K:F]=4$. 比较次数表明$\mathbb{C}(w)=F$. ■

一个称为吕罗特(Lüroth)定理的著名定理断言$\mathbb{C}(y)$的任意真包含复数的子域是 y 的某个

555 有理函数 w 的有理函数域.

第五节 主要定理的证明

设 $f(x)$是一个系数属于域 F 的 n 次首一多项式. 回忆 $f(x)\in F[x]$的分裂域是一个形如 $K=F(\alpha_1, \cdots, \alpha_n)$的域，使得在 $K[x]$中 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$. 分裂域的存在性已在第十三章(5.3)中证明. 现在我们想要证明一个给定多项式 $f(x)$的任意两个分裂域是同构的. 这从形如 $F(\alpha)$的扩域由 α 在 F 上的既约多项式确定这一事实和由某种“记账”得到. 记账对证明的要求在记号上有点混乱，但是不难.

域的任一同构 $\varphi: F \longrightarrow \widetilde{F}$ 通过

$$a_n x^n + \cdots + a_0 \rightsquigarrow \tilde{a}_n x^n + \cdots + \tilde{a}_0$$

(其中$\tilde{a}_i=\varphi(a_i)$)扩张为多项式环之间的同构 $F[x] \longrightarrow \widetilde{F}[x]$. 我们用$\tilde{f}(x)$表示 $f(x)$的象. 由于 φ 是同构，$\tilde{f}(x)$是既约多项式当且仅当 $f(x)$是既约的.

下面的引理推广了第十三章(2.9).

【5.1】引理 *用上面的记号，设 $f(x)$是 $F[x]$的一个既约多项式. 设 α 是 $f(x)$在 F 的一个扩域 K 中的根，并设$\tilde{\alpha}$是$\tilde{f}(x)$在$\widetilde{F}$的一个扩域$\widetilde{K}$中的根. 存在唯一的同构*

$$\varphi_1: F(\alpha) \longrightarrow \widetilde{F}(\tilde{\alpha}),$$

它在 F 上的限制是 φ 且将 α 变到$\tilde{\alpha}$.

证明 我们知道 $F(\alpha)$同构于商 $F[x]/(f)$，且类似地$\widetilde{F}(\tilde{\alpha})$同构于$\widetilde{F}[x]/(\tilde{f})$. 刚才看到环 $F[x]$与$\widetilde{F}[x]$是同构的，并且由于 f 与$\tilde{f}$在这个同构下相对应，因此它们生成的理想(f)与$(\tilde{f})$也在这个同构下相对应. 因而剩余环 $F[x]/(f)$与$\widetilde{F}[x]/(\tilde{f})$也是同构的. 把这些同构合起来就得到所求的同构 φ_1. 因为 α 在 F 上生成 $F(\alpha)$，所以 φ 的扩张是唯一的. ■

【5.2】命题 *设 $\varphi: F \longrightarrow \widetilde{F}$ 是域的同构. 设 $f(x)$是 $F[x]$中的一个非常数多项式，并设$\tilde{f}(x)$是$\widetilde{F}[x]$中对应的多项式. 设 K 和$\widetilde{K}$是 $f(x)$和$\tilde{f}(x)$的分裂域. 则存在一个同构 $\psi: K \longrightarrow \widetilde{K}$，它在 K 的子域 F 的限制为 φ.*

如果令 $F=\widetilde{F}$ 且 $\varphi=$恒等映射，我们得到下面的推论：

【5.3】推论 *$f(x)\in F[x]$在 F 上的任意两个分裂域是同构的.*

556 这个推论是我们真正想要的结果. 命题中引入的辅助同构 φ 使证明的归纳步骤可以进行.

命题(5.2)的证明 如果 $f(x)$在 F 上分解为线性因式的乘积，则$\tilde{f}(x)$也分解为线性因式的乘积. 在这一情形 $K=F$ 且$\widetilde{K}=\widetilde{F}$，因而 $\varphi=\psi$. 假设 f 不完全分裂. 选择 $f(x)$的一个次数>1的既约因式 $g(x)$. 对应的多项式$\tilde{g}(x)$为$\tilde{f}(x)$的一个既约因式. 设 α 是 g 在 K 中的一个根并且记 $F_1=F(\alpha)$. 在$\widetilde{K}$中作一个类似的选择$\tilde{\alpha}$并且令$\widetilde{F}_1=\widetilde{F}(\tilde{\alpha})$. 于是由引理(5.1)，可将 φ 拓广为一

个同构 φ_1：$F_1 \longrightarrow \widetilde{F}_1$，它使 $\alpha \rightsquigarrow \widetilde{\alpha}$. 作为 f 在 F 上的分裂域，K 也是 f 在更大的域 F_1 上的分裂域，同样地 $\widetilde{K}$ 也是 $\widetilde{f}$ 在 $\widetilde{F}_1$ 上的分裂域. 因而可将 F，$\widetilde{F}$，φ 换为 F_1，$\widetilde{F}_1$，φ_1，并且对 K 在 F 上的次数进行归纳进行证明. ■

现在要证明定理中的第二个，即定理(1.11)，它是我们在第一节中提出的. 这个定理的一部分在上一节已利用推论(4.5)加以证明. 为方便起见，我们在这里复述其另一部分.

定理 设 K 是多项式 $f(x)\in F[x]$ 的分裂域. 则 K 是 F 的一个伽罗瓦扩域；即 $|G(K/F)|=[K:F]$.

我们将再过一遍命题(5.2)的证明，通过仔细观察选择的个数来证明这个定理.

【5.4】引理 用(5.2)的记号，拓广 φ 的同构 ψ：$K \longrightarrow \widetilde{K}$ 的个数等于 $[K:F]$.

如果取 $F=\widetilde{F}$，$K=\widetilde{K}$ 且 $\varphi=$恒等映射，则由这个引理就可得到定理.

引理(5.4)的证明 我们像在命题(5.2)的证明中一样进行证明，选择 $f(x)$ 的既约因式 $g(x)$，并选择 $g(x)$ 在 K 中的一个根 α. 设 $F_1=F(\alpha)$. 任意拓广 φ 的同构 ψ：$K \longrightarrow \widetilde{K}$ 将 F_1 映到 $\widetilde{K}$ 的某个子域 $\widetilde{F}_1$. 这个域 $\widetilde{F}_1$ 将具有 $\widetilde{F}(\widetilde{\alpha})$ 的形式，其中 $\widetilde{\alpha}=\psi(\alpha)$ 是 $\widetilde{g}(x)$ 在 $\widetilde{K}$ 中的一个根.

反之，要把 φ 拓广为 ψ，我们可以从选择 $\widetilde{g}(x)$ 在 $\widetilde{K}$ 中的任一个根 $\widetilde{\alpha}$ 开始. 然后通过令 $\varphi_1(\alpha)=\widetilde{\alpha}$ 将 φ 拓广为一个映射 φ_1：$F_1 \longrightarrow \widetilde{F}_1=\widetilde{F}(\widetilde{\alpha})$. 我们在 $[K:F]$ 上用归纳法. 由于 $[K:F_1]<[K:F]$，归纳假设告诉我们对这个特别取定的 φ_1，存在 $[K:F_1]$ 个 φ_1 到同构 ψ：$K \longrightarrow \widetilde{K}$ 的拓广. 另一方面，由于 g 与 $\widetilde{g}$ 是既约的，$\widetilde{g}$ 在 $\widetilde{K}$ 的根互不相同[第十三章(5.8)]. 因而 $\widetilde{\alpha}$ 的选择的个数就是 g 的次数，也就是 $[F_1:F]$. 同构 φ_1 的选法有 $[F_1:F]$ 个. 这总共给出了 $[K:F_1][F_1:F]=[K:F]$ 个 φ 到同构 ψ：$K \longrightarrow \widetilde{K}$ 的拓广. ■

由于多项式 $f(x)\in F[x]$ 的任意两个分裂域 K 是同构的，因此在同构下伽罗瓦群 $G(K/F)$ 只依赖于 f. 常常将它称为 F 上多项式的伽罗瓦群.

557

下面的推论汇集了扩域是伽罗瓦扩域的判别法. 其中大多数已经证明，我们把剩下的证明留作练习.

【5.5】推论 设 K/F 是有限扩域. 下列结论等价：

(i) K 是 F 的伽罗瓦扩域；

(ii) K 是一个既约多项式 $f(x)\in F[x]$ 的分裂域；

(ii′) K 是一个多项式 $f(x)\in F[x]$ 的分裂域；

(iii) F 是伽罗瓦群 $G(K/F)$ 在 K 上作用的不变域；

(iii′) F 是 K 的一个有限自同构群作用的不变域.

我们现在有了足够多的信息来证明伽罗瓦理论的主要定理，它将中间域与伽罗瓦群的子群联系起来.

定理(1.15)的证明 设 K/F 是一个伽罗瓦扩域. 必须证明映射

$$L \rightsquigarrow G(K/L) \quad 和 \quad H \rightsquigarrow K^H$$

是中间域的集合与 $G=G(K/F)$ 的子群的集合之间的互逆的函数．为此，我们验证这两个映射在两个方向的合成是恒等映射．

设 L 是一个中间域．对应的 G 的子群是 $H=G(K/L)$．由定义，H 在 L 上平凡地作用，因而 $L\subset K^H$．另一方面，由(1.13)，K 是 L 的伽罗瓦扩域；因此 $[K:L]=|H|$．由定理(4.6)，$|H|=[K:K^H]$，因而 $L=K^H$．

在另一个方向，假设我们从一个子群 $H\subset G$ 开始，并设 $L=K^H$．则 $H\subset G(K/L)$．但 $|H|=[K:K^H]=[K:L]=|G(K/L)|$．因而 $H=G(K/L)$．这表明两个映射是互逆的，正是我们需要证明的．由于 K 是 $L=K^H$ 的伽罗瓦扩域，因此 $[K:L]=H$，且 $[L:F]=[G:H]$．■

现在讨论主要定理中给出的对应有一些其他细节．首先，域与子群间的对应是反序的，即如果 L，L' 是两个中间域且如果 $H=G(K/L)$，$H'=G(K/L')$ 是对应的子群，则 $L\subset L'$ 当且仅当 $H\supset H'$．由映射的定义这是清楚的，并且与关系(1.16)是一致的．

为了得到完整描述，我们将证明作为 F 的伽罗瓦扩域的那些中间域 L 对应于 G 的正规子群．设 L 是一个中间域．K 的一个 F-自同构 σ 将 L 映到某个中间域 σL，它可能与 L 相同也可能不同．我们称 σL 为一个共轭子域．

【5.6】定理　*设 K/F 是一个伽罗瓦扩域，并设 L 是一个中间域．设 $H=G(K/L)$ 是 $G=G(K/F)$ 中对应的子群．*

558

(a) 设 σ 是 G 的一个元素．G 的对应于共轭子域 σL 的子群是共轭子群 $\sigma H\sigma^{-1}$．换言之，$G(K/\sigma L)=\sigma H\sigma^{-1}$．

(b) L 是 F 的伽罗瓦扩域当且仅当 H 是 G 的正规子群．当这一点成立时，$G(L/F)$ 同构于商群 G/H．

【5.7】图表

$G=G(K/F)$ 在 K 上作用，使 F 不变

K
} $H=G(K/L)$ 在 K 上作用，使 L 不变
L
} 如果 H 正规，则 $G/H=G(L/F)$ 在此作用
F

【5.8】例　在三次方程(2.1)的情形，其分裂域的次数为 6，不是 F 和 K 的仅有的伽罗瓦扩域的中间扩域为 $F(\delta)$，它对应于交错群 $H=A_3\subset S_3$．伽罗瓦群 $G(F(\delta)/F)$ 是 2 阶循环群，也就是商群 S_3/A_3．三个域 $F(\alpha_i)$ 是共轭的．这与 S_3 的三个 2 阶子群是共轭的是一致的．

定理(5.6)的证明　(a) 设 $\sigma L=L'$．如果 τ 是 $H=G(K/L)$ 的一个元素，则 $\sigma\tau\sigma^{-1}$ 属于 $H'=G(K/L')$．要验证这一点，我们必须证明 $\sigma\tau\sigma^{-1}$ 使任意元素 $\alpha'\in L'$ 不变．由 σL 的定义，有 $\alpha\in L$ 使得 $\alpha'=\sigma(\alpha)$．于是 $\sigma\tau\sigma^{-1}(\alpha')=\sigma\tau(\alpha)=\sigma(\alpha)=\alpha'$，这正是所要证的．由 $H'\supset\sigma H\sigma^{-1}$ 及对称，或通过比较元素个数，得到 $H'=\sigma H\sigma^{-1}$．我们刚刚验证的这个事实实际上是群在集合上作用的一般性质[第五章(6.4)]．

(b) 现在假设 H 是正规的. 则对所有 $\sigma\in G$, 有 $H'\supset\sigma H\sigma^{-1}$; 因此 $G(K/L)=G(K/\sigma L)$. 这表明对所有 σ 有 $L=\sigma L$[见(1.9)]. 这样每个 K 上的 F-自同构将 L 映到自身，因此由限制定义一个 L 上的 F-自同构. 这个限制定义一个同态

【5.9】
$$\pi: G\longrightarrow G(L/F).$$
其核是在 L 上导出恒等映射的 $\sigma\in G$ 的集合，也就是 H. 因而 G/H 与 $G(L/F)$ 的子群同构. 比较次数和阶，我们发现
$$[L:F]=|G/H|\leqslant|G(L/F)|.$$
由此得到 L 是伽罗瓦扩域且 $G/H\approx G(L/F)$.

反之，假设 L/F 是伽罗瓦的. 则 L 是某个多项式 $g(x)\in F[x]$ 的分裂域；即 $L=F(\beta_1,\cdots,\beta_k)$，其中 β_i 是 $g(x)$ 在 K 中的根. K 上的 F-自同构 σ 置换这些根因而将 L 映射到自身: $L=\sigma L$. 由(a)，$H=\sigma H\sigma^{-1}$；这样 H 是一个正规子群. ■

559

第六节 四次方程

设 K/F 是伽罗瓦扩域. 我们已看到如果 β 是 K 的一个元素，它在 F 上的首一既约多项式是 $g(x)$，则 g 在 K 上完全分裂，β 的 G-轨道是 g 的根的集合(4.4). 因而只要既约多项式 $g\in F[x]$ 在 K 中至少有一个根，则 G 在这个多项式的根上可迁地作用. 把这个观察与命题(1.14)结合起来，我们得到:

【6.1】命题 *设 K/F 是多项式 $f(x)\in F[x]$ 的分裂域. K/F 的伽罗瓦群 G 在 f 的根的集合 $\{\alpha_1,\cdots,\alpha_n\}$ 上忠实地作用. 因此这个作用将 G 表示成对称群 S_n 的一个子群. 根构成单独一条轨道当且仅当 f 在 F 上既约.*

当伽罗瓦扩域 K 表示为 n 次多项式的分裂域时，通常把伽罗瓦群 G 视为对称群 S_n 的一个子群. 如果多项式 f 是既约的，则它是一个可迁子群，这是指它在指标$\{\mathbf{1},\cdots,\boldsymbol{n}\}$上可迁地作用. 然而同一个伽罗瓦扩域 K/F 可以表示为许多多项式的分裂域，因而 G 的这一作为对称群 S_n 的一个子群的表示不是唯一的.

例如，设 K/F 是使得$[K:F]=6$ 的三次既约方程的分裂域. 则伽罗瓦群表示为整个对称群 S_3. 然而，本原元定理告诉我们 K 可由单独一个元素 γ 生成. 由于$[K:F]=6$，因此 γ 在 F 上的次数为 6. 这表明它的轨道的阶为 6，并且其既约多项式的次数为 6. 因而如果把 K 视为这个六次多项式的分裂域，则伽罗瓦群表示为 S_6 的一个子群. 对表出 S_3 来说这不是一个经济的方法.

假设伽罗瓦扩域 K 是多项式 $f(x)$ 的分裂域并且它在 K 中的根为 $\alpha_1,\cdots,\alpha_n$. 则当将 G 视为 S_n 的一个子群时，我们可以提出下列两个问题:

【6.2】

(i) 给定 S_n 的子群 $\mathcal{H}$，确定是否有 $G\in\mathcal{H}$.

(ii) 求 G.

如果可以对每个子群 $\mathcal{H}$ 解决(i)，则(ii)也可被解决.

拉格朗日解决这些问题的方法是寻找根的那些部分对称的函数. 一个部分对称的多项式是

变量$\{u_1, \cdots, u_n\}$的多项式$p(u_1, \cdots, u_n)$，它在S_n的一个给定子群$\mathcal{H}$中的置换作用下不变，但不在其他置换下不变. 例如，当$n=3$时我们在(2.13)中看到

560

$$(u_1-u_2)(u_1-u_3)(u_2-u_3)$$

是交错群的部分对称函数. 不难通过定义

【6.3】
$$\delta(u)=(u_1-u_2)(u_1-u_3)\cdots(u_{n-1}-u_n)=\prod_{i<j}(u_i-u_j)$$

而将该构造推广到任意的n. 这个元素是判别式(3.6)的平方根. 下标置换的效果是δ乘上置换的符号. 有了这样的部分对称函数，再把多项式的根$\alpha_1, \cdots, \alpha_n$代入其中，就得到$K$的元素$\delta(\alpha)=\delta$,它在根的偶置换下是不变的. 我们可以通过确定判别式D是否是一个元素的平方来确定δ是否属于F. 这将给出关于伽罗瓦群的信息.

【6.4】命题 设K/F是伽罗瓦扩域且它是一个n次既约多项式$f(x)\in F[x]$的分裂域. 设$\alpha_1, \cdots, \alpha_n$是$f(x)$在$K$中的根，并且设$\delta=\delta(\alpha)$. 则$\delta\neq 0$. 而且

(a) $\delta\in F$当且仅当伽罗瓦群G是交错群A_n的子群.

(b) 在任何情形，G的子群$G(K/F(\delta))$总包含在交错群中.

证明 $\delta=0$的情形只有当两个根相等时才会出现，而如果f既约这是不会发生的[第十三章(5.8)]. 其次假设$\delta\in F$. 由于奇置换使$\delta \rightsquigarrow -\delta$且由于$\delta\neq 0$，奇置换不能使$\delta$不变. 另一方面，$F$的元素在$G$中的每个自同构之下不变. 从而得到$G$不能包含奇置换，因此$G\subset A_n$. 反之，如果$\delta\notin F$，我们用$K^G=F$这一事实. G中必有元素不能使δ不变. 这个元素将是个奇置换，因而$G\not\subset A_n$. 这证明了(a). 当用$F(\delta)$代替F时我们由(a)得到(b). ■

现在讨论四次方程，我们从一个由判别式所控制的有趣的特殊情形开始. 考虑表示为嵌套平方根的复数，比如$\alpha=\sqrt{r+s\sqrt{t}}$，其中$r, s, t$属于域$F$. 数

【6.5】
$$\sqrt{3+2\sqrt{2}},\quad \sqrt{5+\sqrt{21}},\quad \sqrt{7+2\sqrt{5}},\quad \sqrt{5+2\sqrt{5}}$$

是一些例子. 我们提出下面的问题：是否存在α的一个是互不嵌套的两个平方根的表达式?

由于$\alpha^2=r+s\sqrt{t}$，容易写出以α为根的一个四次多项式

【6.6】
$$f(x)=(x^2-(r+s\sqrt{t}))(x^2-(r-s\sqrt{t}))=x^4+bx^2+c,$$

其中$b=-2r$而$c=r^2-s^2t$. 如果α'表示$r-s\sqrt{t}$的两个平方根之一，则这个四次多项式的根为

561

【6.7】
$$\alpha, \alpha', -\alpha, -\alpha'.$$

f的分裂域$K=F(\alpha, \alpha')$可由顺序添加三个平方根$\sqrt{t}$，α，α'得到，因而次数$[K:F]$整除8. 如果平方根的添加中有一个不是必须的，则次数将小于8.

我们必须确定f是否既约. 为此，首先检查根为α^2，α'^2的二次多项式$q(y)=y^2+by+c$的可约性. 如果q既约，则f在F中没有根. 在这一情形，如果f可约，它将是两个二次多项式的乘积. 用待定系数法计算，我们发现乘积必有形式

【6.8】
$$x^4+bx^2+c=(x^2+ux+v)(x^2-ux+v).$$

至少在$F=\mathbb{Q}$时，我们能确定是否存在这样的分解.

如果f是可约的，则α是一个二次多项式的根，因而它可以仅用一个平方根写出. 例如，

$\sqrt{3+2\sqrt{2}}$就是这样的情形，它的平方根等于$1+\sqrt{2}$，这可以通过对两个表达式取平方验算得到.(6.5)中其他的例子导出的四次多项式在$\mathbb{Q}$上是既约的.

现在回到我们的问题.假定f是既约的.注意将α用两个互不嵌套的平方根$\sqrt{p}$，$\sqrt{q}$写出相当于求F上一个包含α的双二次扩域$K=F[\sqrt{p},\sqrt{q}]$.假设可以找到一个包含α的双二次扩域K.则K是F的伽罗瓦扩域，因而$f(x)$在K中分解成为线性因式.这表明K包含f的一个分裂域.事实上，因为f既约且次数为4，所以K就是分裂域.因而f的伽罗瓦群G是克莱因四元群.如果G不是克莱因四元群，则α不能用互不嵌套的平方根写出.

反之，如果K/F是其伽罗瓦群为克莱因四元群的伽罗瓦扩域，则K包含三个在F上次数为2的中间域.这些域中的任意两个合起来就生成K.因而K是F的双二次扩域，且K中任意元素可以用互不嵌套的平方根写出.

我们用(6.7)列出的根来计算$f(x)$的判别式.

$$D=\prod_{i<j}(\alpha_i-\alpha_j)^2=(4\alpha\alpha')^2(\alpha-\alpha')^4(\alpha+\alpha')^4=2^4(b^2-4c)^2c=2^8s^4t^2(r^2-s^2t).$$

如果D在F中为一个平方数，则G是交错群A_4的可迁子群，其阶整除8.克莱因四元群是仅有的这样的群.它由2阶偶置换构成：

【6.9】 $$V=\{(\mathbf{1}),(\mathbf{12})(\mathbf{34}),(\mathbf{13})(\mathbf{24}),(\mathbf{14})(\mathbf{23})\}.$$

V在$\{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4}\}$上没有其他可迁的作用.因而我们得到：

【6.10】命题 *设$\alpha=\sqrt{r+s\sqrt{t}}$，其中$r,s,t\in F$，并且假设$f(x)=x^4-2rx^2+(r^2-s^2t)$在$F$上既约.则$\alpha$可以用两个互不嵌套的平方根写出当且仅当$r^2-s^2t$是$F$中的平方数.*

[562]

如果$\alpha=\sqrt{5+\sqrt{21}}$，则$r^2-s^2t=25-21=4$是一个平方数.在(6.5)的最后两个例子中，$r^2-s^2t$不是$\mathbb{Q}$中的平方数.

我们具体确定$\alpha=\sqrt{5+\sqrt{21}}$的非嵌套表达式.伽罗瓦理论提供了线索，也就是它建议确定中间域.它们是$\mathbb{Q}$的二次扩域，因而它们由平方根生成.这些平方根是我们表达α所需要的.有一个中间域是明显的，也就是$\mathbb{Q}[\sqrt{21}]$.但这不是我们所需要的.为求其他中间扩域，我们确定由$\sigma=(\mathbf{12})(\mathbf{34})$生成的2阶子群$H$的不变域.如果$f$的根按(6.7)的顺序排列，则$\alpha$的$H$-轨道是$\{\alpha,\alpha'\}$,(其中$\alpha'=\sqrt{5-\sqrt{21}}$，且$\alpha$在$K^H$上的既约多项式为$(x-\alpha)(x-\alpha')=x^2-(\alpha+\alpha')x+\alpha\alpha'$.)因而$K$在域$L=F(\alpha+\alpha',\alpha\alpha')$上的次数为2，并且这个域包含在$K^H$中.对次数进行比较表明$L=K^H$.用这个线索，我们计算得到$\alpha\alpha'=2$，$(\alpha+\alpha')^2=14$，因而$\alpha+\alpha'=\sqrt{14}$.同样地，$\alpha-\alpha'=\sqrt{6}$.解出$\alpha$，得到$\alpha=\frac{1}{2}(\sqrt{6}+\sqrt{14})$.

分析一般的四次方程是很困难的，其根通常都无法以一种有用的方式具体写出.然而存在另一个部分对称函数，它有助于确定伽罗瓦群.令$f(x)$是在分裂域K中的根为$\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}$的四次既约多项式.于是由命题(6.1)，其伽罗瓦群是S_4的子群，且根构成一条轨道.S_4的可迁子群为

【6.11】 $$S_4,A_4,D_4,C_4,V,$$

其中 V 是群(6.9). 实际上，有三个与 D_4 同构的共轭子群和三个与 C_4 同构的共轭子群. 其他的子群是唯一确定的. S_4 还有一些其他的子群同构于克莱因四元群，但它们不是可迁的.

我们来求能区分这些子群的根的部分对称函数，我们已看到，元素 δ 确定是否有 $G \subset A_4$. 我们列出的 A_4 的子群是 A_4 和 V. 因而 $\delta \in F$ 当且仅当 G 是这三个群之一.

其次，考虑部分对称多项式

【6.12】
$$\beta_1(u) = u_1u_3 + u_2u_4$$

下标的置换将 $\beta_1(u)$ 变为三个多项式 $\beta_i(u)(i=1, 2, 3)$ 之一，其中

$$\beta_2(u) = u_1u_2 + u_3u_4 \quad 而 \quad \beta_3(u) = u_1u_4 + u_2u_3.$$

由于 S_4 的阶为 24，所以 $\beta_1(u)$ 的稳定子的阶为 8；它是三个二面体群 D_4 之一. 多项式 $(x-\beta_1(u))(x-\beta_2(u))(x-\beta_3(u))$ 在变量 u_i 的所有置换下都是不变的，因而其系数为对称函数. 可以用初等对称函数把它们具体计算出来.

563

回到我们的四次多项式，把根 α_i 代入 $\beta_j(u)$，得到三个元素 $\beta_j(\alpha)=\beta_j \in K$. 它们构成对称群在根的作用下的一条轨道. 如果它们是 K 中互不相同的元素，则 β_1 在 S_4 中的稳定子的阶为 8，因而它将是二面体群 D_4. 幸运的是：β_j 的确是互不相同的. 例如，

$$\beta_1 - \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 = (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2).$$

由于我们假定 f 是既约的，因此其根 α_i 是互不相同的. 等式的右边表明 $\beta_1 - \beta_2 \neq 0$.

由于伽罗瓦群 G 置换元素 β_i，因而多项式 $g(x)=(x-\beta_1)(x-\beta_2)(x-\beta_3)$ 的系数属于 F，称之为四次多项式 $f(x)$ 的三次预解式.

虽然对称群在 $\{\beta_1, \beta_2, \beta_3\}$ 上的作用是可迁的，但作为 S_4 的子群，伽罗瓦群 G 的作同可能是不可迁的. 不论它是否可迁，都提供了 G 的信息. 例如，如果 G 使 β_1 不变，则 G 包含在 β_1 的稳定子 D_4 之中. 在这一情形，β_1 将属于域 F(1.9)，因而三次预解式在 F 中有根. 如命题(6.4)的证明一样，我们得到下面的命题：

【6.13】命题 *设 $g(x)$ 是四次既约多项式 $f(x)$ 的三次预解式，并设 K 是 f 的分裂域. 则 $g(x)$ 在 F 中有根当且仅当伽罗瓦群 $G=G(K/F)$ 是二面体群 D_4 中的一个的子群. 无论如何，如果 β 是 $g(x)$ 在 K 中的根，则伽罗瓦群 $G(K/F(\beta))$ 是二面体群 D_4 中的一个子群.*

这样多项式 x^2-D(其中 D 是判别式)加上三次预解式就差不多足以描述伽罗瓦群了. 结果总结在下表中：

【6.14】表

	D 是 F 中平方数	D 不是 F 中平方数
g 可约	$G=V$	$G=C_4$ 或 D_4
g 既约	$G=A_4$	$G=S_4$

任意的四次方程的具体计算不是一件令人愉快的事，但我们容易计算形如

【6.15】
$$x^4 + rx + s$$

的四次多项式的判别式. 这个判别式是一个 12 次的对称多项式，因而是初等对称函数 $s_1, \cdots, s_4$ 的带权次数为 12 的多项式. 在判别式的未知公式里用 $(0, 0, -r, s)$ 代入 (s_1, s_2, s_3, s_4) 会

使得任意涉及 s_1 或 s_2 的单项式为零．不涉及 s_1 和 s_2 的带权次数为 12 的单项式仅有 s_3^4 和 s_4^3．因而(6.15)的判别式具有形式

564

$$D = \Delta(0,0,-r,s) = cr^4 + c's^3.$$

我们可以通过计算两个特殊多项式的判别式来确定系数 c，c'．答案是

【6.16】 $$D = -27r^4 + 256s^3.$$

例如，

【6.17】 $$f(x) = x^4 + 8x + 12$$

的判别式为 $3^4 \cdot 2^{12}$．这是$\mathbb{Q}$中的平方数．因而多项式(6.17)在$\mathbb{Q}$上的分裂域的伽罗瓦群是 A_4 的子群．

要计算多项式(6.15)的三次预解式 $g(x)$，我们将根为 u_1，…，u_4 的一般多项式的三次预解式记作

$$g(x) = x^3 - b_1x^2 + b_2x - b_3;$$

则由于 β_i 是$\{u_j\}$的二次函数，b_i 关于$\{u_j\}$的次数为 $2i$ 并且关于对称函数的带权次数为 $2i$．如上面一样，可以得到

【6.18】 $$g(x) = x^3 - 4sx - r^2.$$

特殊的四次多项式(6.17)的三次预解式是 $x^3-48x-64$．四次多项式(6.17)和其三次预解式都在$\mathbb{Q}$上既约．由此得到对多项式(6.17)有 $G=A_4$．

第七节 库默尔扩域

考虑域 F 上一个形如

【7.1】 $$f(x) = x^p - a$$

的多项式的分裂域，其中 p 是素数．假设基域 F 是$\mathbb{C}$的子域并且它包含 p 次本原单位根 $\zeta_p = e^{2\pi i}/p$．$f(x)$的复根是 a 的 p 次根，如果 α 是一个特定的 p 次根，则 $f(x)$的根是

【7.2】 $$\alpha, \zeta\alpha, \zeta^2\alpha, \cdots, \zeta^{p-1}\alpha,$$

其中 $\zeta=\zeta_p$．因而分裂域由单独一个根生成：$K=F(\alpha)$．

【7.3】命题 *设 F 是$\mathbb{C}$中包含 p 次单位根 ζ_p 的子域，并设 a 是 F 的元素，它不是 F 中的 p 次幂．则 $f(x)=x^p-a$ 的分裂域在 F 上的次数为 p 且其伽罗瓦群是 p 阶循环群．*

证明 设 K 是 f 的分裂域，并设 α 是它在 K 中的一个根．假设 α 不属于 F．则存在 K/F 的自同构 σ，它不能保持 α 不变．由于 f 的根为 $\zeta^i\alpha$，$i=0$，…，$p-1$，因而对某个 $\nu\neq 0$ 有 $\sigma(\alpha)=\zeta^\nu\alpha$．现在计算 σ 的幂．记住 σ 是个自同构且因为 $\zeta\in F$，有 $\sigma(\zeta)=\zeta$，我们得 $\sigma^2(\alpha)=\sigma(\zeta^\nu\alpha)=\zeta^\nu\sigma(\alpha)=\zeta^{2\nu}\alpha$．同样地，对每个 i 都有 $\sigma^i(\alpha)=\zeta^{i\nu}\alpha$．由于 ζ 是 p 次单位根，因而使 α 不变的 σ 的最小正幂是 σ^p．因此 σ 在伽罗瓦群中的阶至少为 p．另一方面，α 在 F 上生成 K，且 α 是 p 次多项式 $f(x)=x^p-a$ 的根，因而$[K:F]\leqslant p$.这同时也证明了$[K:F]=p$，$f(x)=x^p-a$ 在 F 上既约以及 $G(K/F)$是 p 阶循环群． ■

565

下面是命题(7.3)的一个令人惊讶的逆：

【7.4】定理 *设 F 是$\mathbb{C}$的包含 p 次单位根 ζ 的子域，并设 K/F 是次数为 p 的伽罗瓦扩域．则*

K 由在 F 上添加一个 p 次根得到.

这一类型的扩域通常称为库默尔扩域. 对 $p=2$，定理成为我们熟悉的断言：每个二次扩域可通过添加一个平方根得到. 但假定 $p=3$ 且 F 包含 ζ_3. 如果三次既约多项式(2.3)的判别式是 F 中的平方，则 f 的分裂域的次数为 3[见(2.16)]，因而其伽罗瓦群为循环群. 因此这样的多项式的分裂域具有 $F(\sqrt[3]{a})$ 的形式，其中 $a\in F$. 这并不是明显的.

定理(7.4)的证明 伽罗瓦群 G 的阶为素数 $p=[K:F]$，因而它是循环群. 任意不是单位元的元素 σ 都会生成它. 我们将 K 视为 F-向量空间. 则 σ 是 K 上的一个线性算子. 这是因为由于 σ 是 F-自同构，对所有的 $c\in F$ 及 $\alpha, \beta\in K$，有

$$\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta) \quad 和 \quad \sigma(c\alpha)=\sigma(c)\sigma(\alpha)=c\sigma(\alpha).$$

由于 G 是 p 阶循环群，故 $\sigma^p=1$. 这个算子的特征值 λ 必满足条件 $\lambda^p=1$，这表明 λ 是 ζ 的一个幂. 由假设，这些特征值属于域 F. 而且至少有一个特征值不等于 1. 这是关于 T 的任意某个幂为恒等映射的线性算子的一个事实，因为这样的线性算子可以对角化[第九章(2.3)]. 它的特征值是表示它的对角矩阵 A 的那些元素. 如果像在这里的一样，T 不是恒等映射，则 $A\neq I$，因而它的某个对角元素不等于 1.

我们选择特征值 $\zeta^i\neq 1$ 的一个特征向量 α. 则 $\sigma(\alpha)=\zeta^i\alpha$，因此 $\sigma(\alpha^p)=\sigma(\alpha)^p=(\zeta^i\alpha)^p=\zeta^{ip}\alpha^p=\alpha^p$. 这样 σ 使 α^p 不变. 由于 σ 生成 G，元素 α^p 属于不变域 K^G，也就是 $F(1.9)$. 因而我们找到一个 p 次幂属于 F 的元素 $\alpha\in K$. 由于 $\sigma(\alpha)\neq\alpha$，故 α 本身不属于 F. 由于$[K:F]$是素数，因此 α 生成 K. ∎

【7.5】例 考虑三次循环多项式(2.12)x^3-3x+1. 设$\{\eta_1, \eta_2, \eta_3\}$表示它的根. 存在一个元素 566 $\sigma\in G(K/F)$作为循环置换作用. 选择 K 在 $F=\mathbb{Q}(\zeta_3)$上的一个基$(1, \eta_1, \eta_2)$. (为什么这是一个基?)线性算子 σ 关于这个基的矩阵是

$$\sigma=\begin{bmatrix}1&0&0\\0&0&-1\\0&1&-1\end{bmatrix},$$

这是因为 $\sigma(1)=1$，$\sigma(\eta_1)=\eta_2$，$\sigma(\eta_2)=\eta_3=-\eta_1-\eta_2$. 向量$(0, 1, -\zeta_3)^t$ 是以 ζ_3 为特征值的特征向量. 这样如果 $\alpha=\eta_1-\zeta_3\eta_2$，则 α^3 是 F 的一个元素，且 α 生成 x^3-3x+1 在 F 上的分裂域. 可以用 $\eta_1=\zeta_9+\zeta_9^{\,8}$ 及 $\eta_2=\zeta_9^{\,2}+\zeta_9^{\,7}$ 具体计算 α^3. 注意 $\zeta_3=\zeta_9^{\,3}$，我们得到 $\alpha=\zeta_9^{\,8}-\zeta_9^{\,5}$ 和 $\alpha^3=3(1-\zeta_3)$.

【7.6】例 设 $f(x)$是域 F 上的任意一个三次既约多项式，并设 K 是 $f(x)(x^3-1)$在 F 上的分裂域. 设 $L\subset K$ 是由 ζ 和 $\delta=\sqrt{D}$生成的中间域，其中 D 是 f 的判别式. 则由(2.16)，$[L:F]$整除 4 且$[K:L]=3$. 无论如何，四个元素$\{1, \sqrt{D}, \sqrt{-3}, \sqrt{(-3D)}\}$都张成 F-向量空间 L. 由定理(7.4)，存在 $b\in L$ 使得 $K=L(\sqrt[3]{b})$. 因而 $f(x)$的根可以写为形如

$$\sqrt[3]{c_1+c_2\sqrt{D}+c_3\sqrt{-3}+c_4\sqrt{-3D}}, \quad c_i\in F$$

的三次根的表达式.

第八节 分圆扩域

复数中在$\mathbb{Q}$上由 $\zeta_n=e^{2\pi i/n}$生成的子域 K 称为一个分圆域. 并且对$\mathbb{C}$的任意子域 F，域 $F(\zeta_n)$称为 F 的分圆扩域. 它是多项式

【8.1】
$$x^n-1$$
在 F 上的分裂域. 如果用 ζ 表示 ζ_n，则这个多项式的根为 ζ 的幂，也就是 n 次单位根 1，ζ，ζ^2，…，ζ^{n-1}. 本节我们将专注于 n 为不等于 2 的素整数 p 的情形.

多项式 $x^{p-1}+\cdots+x+1$ 在$\mathbb{Q}$上是既约的，且 $\zeta=\zeta_p$ 是它的一个根[第十一章(4.6)]. 因而它是 ζ 在$\mathbb{Q}$上的既约多项式. 它的根是 ζ，ζ^2，…，ζ^{p-1}. 因此$\mathbb{Q}(\zeta)$在$\mathbb{Q}$上的伽罗瓦群的阶为 $p-1$.

【8.2】命题 *设 p 是素整数，并设 $\zeta=\zeta_p$.*

(a) $\mathbb{Q}(\zeta)$在$\mathbb{Q}$上的伽罗瓦群同构于素域$\mathbb{F}_p$ 的非零元素的乘法群$\mathbb{F}_p^\times$. 它是 $p-1$ 阶循环群.

(b) 对$\mathbb{C}$的任意子域 F，$F(\zeta)$在 F 上的伽罗瓦群是循环群.

567

证明 设 G 是 $F(\zeta)$在 F 上的伽罗瓦群. 我们如下定义一个映射 v：$G\longrightarrow\mathbb{F}_p^\times$：设 $\sigma\in G$ 是一个自同构. 它将 ζ 映到多项式 $x^p+\cdots+x+1$ 的另一个根，比如映到 ζ^i. 因为 ζ 的乘法的阶为 p，所以幂 i 作为一个模 p 的整数是唯一确定的. 令 $v(\sigma)=i$. 我们验证 v 是保持乘法的：如果τ是 G 的另一个元素且有 $v(\tau)=j$，即$\tau(\zeta)=\zeta^j$，则

【8.3】
$$\sigma\tau(\zeta)=\sigma(\zeta^j)=\sigma(\zeta)^j=\zeta^{ij}.$$
而且恒等自同构将 ζ 映为 ζ，因此 $v(1)=1$. 由于 v 与乘法相容并且 $v(\sigma)\neq 0$，因此 v 是到$\mathbb{F}_p^\times$的一个同态. 由于 ζ 生成 K，当知道一个自同构在 ζ 上的作用时，它在整个的作用便是唯一确定的，因而我们的同态是单射. 这样 G 同构于它在$\mathbb{F}_p^\times$ 中的象. 由于$\mathbb{F}_p{}^\times$是循环群，它的每个子群也是循环群. 因而 G 是循环群. 如果 $F=\mathbb{Q}$，则 $|G|=|\mathbb{F}_p{}^\times|=p-1$，因而两个群是同构的. ■

假设 $F=\mathbb{Q}$. 则对每个整除 $p-1$ 的整数 k，作为 $p-1$ 阶循环群，$K=\mathbb{Q}(\zeta_p)$的伽罗瓦群 G恰有一个 k 阶子群. 如果 $p-1/k=r$ 且如果σ 是G 的一个生成元，则 k 阶子群由σ^r 生成. 因而由伽罗瓦理论的主要定理，恰好有一个中间域 L 使$[L:\mathbb{Q}]=r$. 这些域由某些 $\zeta=\zeta_p$ 的幂的和生成. 我们将用一些简单的例子说明这一点.

最简单的情形为 $p=5$. 于是$[K:\mathbb{Q}]=4$，并且存在一个$\mathbb{Q}$上的次数为 2 的中间域. 它由 $\eta=\zeta+\zeta^4=2\cos 2\pi/5$生成. 由于 $2\cos 2\pi/5=\frac{1}{2}(-1+\sqrt{5})$，因此中间域是二次数域$\mathbb{Q}(\sqrt{5})$.

【8.4】命题 *在$\mathbb{Q}$上次数为$\frac{1}{2}(p-1)$的 $K=\mathbb{Q}(\zeta_p)$的子域 L 是由元素 $\eta=\zeta+\zeta^{p-1}=2\cos 2\pi/p$ 在$\mathbb{Q}$上生成的. 而且 $L=K\cap\mathbb{R}$.*

由于 $L=K\cap\mathbb{R}$，L 也称为 K 的实子域.

证明 注意到 ζ 是二次多项式 $x^2-\eta x+1$ 的根，它的系数属于$\mathbb{Q}(\eta)$. 因而$[K:\mathbb{Q}(\eta)]\leqslant 2$. 另一方面，$\eta$ 是实数而 ζ 不是，因而$\mathbb{Q}(\eta)<K$. 从而得到$[K:\mathbb{Q}(\eta)]=2$，$\mathbb{Q}(\eta)=K\cap\mathbb{R}$，且有$[\mathbb{Q}(\eta):\mathbb{Q}]=\frac{1}{2}(p-1)$. ■

当 $p=7$ 时，$\eta=\zeta+\zeta^6$ 在$\mathbb{Q}$上的次数为 3. 它在$\mathbb{Q}$上的既约多项式可用我们在(2.12)之前所使用的方法算出. 我们猜想它的其他根为 $\eta_2=\zeta^2+\zeta^5$ 和 $\eta_3=\zeta^3+\zeta^4$. 这些是其他的 p 次根与其逆的和. 不难证明$\{\eta_1, \eta_2, \eta_3\}$是 $\eta=\eta_1$ 的 G-轨道，因而可以形式地证明这个猜想成立. 展开$(x-\eta_1)(x-\eta_2)(x-\eta_3)$并利用关系 $\zeta^6+\cdots+\zeta+1=0$，我们得到 η 在$\mathbb{Q}$上的既约多项式 x^3+x^2-2x-1.

568

分圆域$\mathbb{Q}(\zeta_7)$也包含$\mathbb{Q}$的一个二次扩域．它由$\varepsilon=\zeta+\zeta^2+\zeta^4$生成．如果令$\varepsilon'=\zeta^3+\zeta^5+\zeta^6$，则$(x-\varepsilon)(x-\varepsilon')=x^2+x+2$是它的既约多项式．这个多项式的判别式是$-7$，因而$\mathbb{Q}(\varepsilon)=\mathbb{Q}(\sqrt{-7})$．因此$\mathbb{Q}(\zeta_7)$包含$\sqrt{-7}$．

假设$p=17$．则$[\mathbb{Q}(\zeta):\mathbb{Q}]=16$．一个16阶的循环群包含子群链$C_{16}\supset C_8\supset C_4\supset C_2\supset C_1$．由伽罗瓦理论的主要定理，存在$\mathbb{Q}$上次数为1，2，4，8，16的对应的中间域链$\mathbb{Q}\subset F_1\subset F_2\subset F_3\subset\mathbb{Q}(\zeta)$．如命题(8.4)所指出的，8次域$F_3$是由$\eta=2\cos 2\pi/17$生成的实子域．由于这个链中每个扩域的次数都是2，因此F_3可由逐步添加三个平方根得到．这证明$2\cos 2\pi/17$(因而正17边形)是可以用直尺和圆规作出的[第十三章(4.9)]．

567

我们将对所有素数描述的另一个扩域是在$\mathbb{Q}$上次数为2的扩域．伽罗瓦理论的主要定理告诉我们$\mathbb{Q}$上只有唯一一个次数为2的中间域，它对应于G的阶为$\frac{1}{2}(p-1)$的子群H．如果G由σ生成，则H由σ^2生成．

【8.5】定理 设p是个奇素数，L是$\mathbb{Q}$的包含在分圆域$\mathbb{Q}(\zeta_p)$中的唯一的二次扩域．则

$$L=\mathbb{Q}(\sqrt{\pm p}),$$

其中符号为$(-1)^{1/2(p-1)}$．

证明 我们需要选出一个容易确定其方程的L的生成元．高斯的方法是取适当选择的ζ的幂的一半之和．

还有一个稍微容易一点的L的生成元的选择．设D是多项式

【8.6】
$$x^p-1$$

的判别式．这个判别式虽然可以直接用根$\{1,\zeta,\zeta^2,\cdots,\zeta^{p-1}\}$算出，但使用下面这个漂亮的公式来求判别式$D$更为容易：

【8.7】引理 设$f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$．则$f$的判别式为

$$D=\pm f'(\alpha_1)\cdots f'(\alpha_n)=\pm\prod_i f'(\alpha_i),$$

其中f'是f的导数．

证明 由求导乘积法则，

$$f'(x)=\sum_{i=1}^{n}(x-\alpha_1)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_n).$$

因而

$$f'(\alpha_i)=(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n).$$

569 这是由给定的i及$j\neq i$与$(\alpha_i-\alpha_j)$的积．这样

$$\prod_i f'(\alpha_i)=\prod_{i\neq j}(\alpha_i-\alpha_j)=\pm D.$$ ■

我们对多项式x^p-1应用这个引理，其导数是px^{p-1}，因而判别式为

$$D=\pm\prod_i p\zeta^{i(p-1)}=\pm\zeta^N p^p,$$

其中幂N是一个整数．要确定ζ^N，我们注意由于x^p-1的系数是有理数，因此D是个有理数．ζ的幂中仅有的有理数为1．因而$\zeta^N=1$且

【8.8】
$$D=\pm p^p.$$
这个判别式的平方根为 $\delta=\sqrt{\pm p^p}$. 它属于域$\mathbb{Q}(\zeta)$. 由于 p 是奇数且由于平方因子可由根号中提出，因而

【8.9】
$$\mathbb{Q}(\delta)=\mathbb{Q}(\sqrt{\pm p}).$$
因此这个域是$\mathbb{Q}(\zeta)$的二次子域，且由于 L 是仅有的二次子域，因此它是 L. 我们将符号的确定留作练习.

最早由克罗内克提出的下面这个定理是代数数论中最漂亮的定理之一. 遗憾的是，在这里要证明它会需要太长的篇幅.

【8.10】定理 *每个$\mathbb{Q}$上伽罗瓦群为阿贝尔群的伽罗瓦扩域 K 包含于某个分圆域$\mathbb{Q}(\zeta_n)$中.*

第九节 五次方程

伽罗瓦工作背后的主要动机是求解五次方程的问题. 我们在本节研究他的解法. 在他之前不久，阿贝尔证明了变系数 a_i 的五次方程

【9.1】
$$x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$$
不能用根式求解，但仍需找到不能用根式求解的一个具体的有理系数的多项式. 无论如何，因为当时这个问题已有 200 多年的历史，大家对它的兴趣一直不减. 此间，伽罗瓦的思想实际上比激发出这些思想的问题要重要得多.

一个用根式的表达式可能会变得非常复杂，我对一般情形也没有一个好的记号. 然而，容易给一个精确的递归定义. 设 F 是复数的任一子域. 我们说复数 α 在 F 上*可用根式表出*，如果存在$\mathbb{C}$的一个子域塔 $F=F_0\subset F_1\subset\cdots\subset F_r$ 使得 [570]

【9.2】

(i) $\alpha\in F_r$，而且

(ii) 对每个 $j=1,\cdots,r$，F_j 在 F_{j-1}上由一个根 β_j 生成. 换句话说，$F_j=F_{j-1}(\beta_j)$，并且对某个整数 n_j 有 $\beta_j^{n_j}\in F_{j-1}$.

这个定义在形式上类似于可由直尺和圆规作出的实数的描述[第十三章(4.9)]. 该描述中只允许有正实数的平方根出现.

【9.3】命题 *设 α 是次数$\leqslant 4$ 的多项式 $f(x)\in F[x]$的一个根，则 α 在 F 上可用根式表出.*

证明 对二次多项式，这是二次公式. 对三次多项式，卡尔达诺公式给出了解答. 假定 $f(x)$是四次多项式. 如果 f 可约，则 α 是次数较低的多项式的一个根，问题已解决. 否则，f 在其分裂域 K 中有不同的根，因而其判别式 D 不为零. 设 $g(x)$是 f 的三次预解式. 我们通过添加 D 的平方根 δ，得到一个域 F_1(可能等于 F). 然后用卡尔达诺公式解出三次预解式. 这将会需要一个平方根扩张 F_2 再跟上一个立方根扩张 F_3. 在此，表(6.14)表明 K/F_3 的伽罗瓦群是克莱因四元群的子群. 因而最多再用两个平方根扩张的序列 $F_3\subset F_4\subset F_5\subset K$ 就达到了 K. ■

在用根式表出时，允许使用 n 次单位根 $\zeta_n=e^{2\pi i/n}$. 而且如果 $n=rs$，则$\sqrt[n]{b}=\sqrt[r]{\sqrt[s]{b}}$. 因此以增

加更多的域链的步数为代价，对于不同的素整数 p，我们可以假定所有的根都是 p 次单位根.

注意在用根式表出时有很大的不确定性，因为每个$\sqrt[n]{b}$都有 n 种选择．记号$(-3+\sqrt[5]{2})^{\frac{1}{4}}$可以表示 20 个复数中的任何一个，因而域塔$\mathbb{Q}\subset\mathbb{Q}(\sqrt[5]{2})\subset\mathbb{Q}((-3+\sqrt[5]{2})^{\frac{1}{4}})$不是唯一确定的．这种不确定性是记号所固有的．由于记号很麻烦，我们也懒得把它搞得更加精确．这些记号也不会用得太多.

【9.4】命题　设 $f(x)$是域 F 上的一个既约多项式．如果 f 在 K 中的一个根可以用根式表出，则其他任何一个根也可以.

证明　假设一个根 α 可以用根式表出，比如通过域塔 $F=F_0\subset\cdots\subset F_r$ 表出．选择一个包含 F_r 且是在 F 上形如 $f(x)g(x)$的多项式的分裂域 L．则 L 也是 fg 在 $F(\alpha)$上的分裂域．设 α' 是 f 在另一个域 K'中的一个根，并设 L'是 fg 在 $F(\alpha')$上的分裂域．则我们可将同构 $F(\alpha)\longrightarrow F(\alpha')$拓广为一个同构 $\varphi:L\longrightarrow L'$(5.2)．域塔 $F=\varphi(F_0)\subset\cdots\subset\varphi(F_r)$表明 α'可以用根式表出. ■

571

【9.5】命题　设 α 是在 F 上可以用根式表出的复数．则可找到域塔 $F=F_0\subset\cdots\subset F_r=K$，使之满足(9.2)的条件(i)和(ii)，并且还有

(iii)对每个 j，F_j 是 F_{j-1} 的伽罗瓦扩域且伽罗瓦群 $G(F_j/F_{j-1})$是循环群.

证明　考虑定义(9.2)中给出的域塔，其中 $F_r=F(\beta_1,\cdots,\beta_r)$．如我们前面所说，可假定存在某个素数 p_j 使 $\beta_j^{p_j}\in F_{j-1}$．设 $\zeta_{p_j}=e^{2\pi i/p_j}$是 p_j 次单位根．我们通过顺序添加元素$(\zeta_{p_1},\cdots,\zeta_{p_r};\beta_1,\cdots,\beta_r)$构成一个新的域链．定理(7.4)和命题(8.2)表明这些扩域中的每一个都是伽罗瓦的，且具有循环伽罗瓦群．由于冗余，这个塔的某些扩张会是平凡的．如果这样，我们就可以缩短域链．由于链中的最后一个域 $F(\{\zeta_{p_j}\},\{\beta_j\})$包含域 F_r，因此它也包含 α. ■

我们考虑 F 上多项式乘积 $f(x)g(x)$的伽罗瓦群．设 K'是 fg 的一个分裂域．则因为 f 在 K'中分解为线性因式的乘积，于是 K'包含 f 的一个分裂域 K．同样地，K'包含 g 的一个分裂域 F'．因而我们得到域的图

【9.6】

$$\begin{array}{ccc} & K' & \\ \cup & & \cup \\ K & & F' \\ \cup & & \cup \\ & F & \end{array}$$

【9.7】命题　使用上面的记号，设 $G=G(K/F)$，$H=G(F'/F)$，$\mathcal{G}=G(K'/F)$.

(a) G 和 H 是$\mathcal{G}$的商群.

(b) $\mathcal{G}$同构于积群 $G\times H$ 的一个子群.

证明　第一个断言由 K 和 F'是中间域且是 F 的伽罗瓦扩域这一事实得到(5.7b)．我们用下标表示典范同态$\mathcal{G}\longrightarrow G$，$\mathcal{G}\longrightarrow H$：$\sigma\rightsquigarrow\sigma_f$ 和 $\sigma\rightsquigarrow\sigma_g$．于是 σ_f 描述 σ 在 f 的根上的作用方式，而 σ_g 描述 σ 在 g 的根上的作用方式．通过 $\sigma\rightsquigarrow(\sigma_f,\sigma_g)$，我们将$\mathcal{G}$映到 $G\times H$．如果 σ_f 和 σ_g 都是恒等映射，则 σ 在 fg 的根上平凡地作用，因此 $\sigma=1$．这表明映射$\mathcal{G}\longrightarrow G\times H$是单射，因而$\mathcal{G}$同构于 $G\times H$ 的子群. ■

572

【9.8】命题　设 f 是 F 上的伽罗瓦群为非阿贝尔单群的多项式．设 F'是 F 的具有阿贝尔伽罗

瓦群的伽罗瓦扩域．设 K' 是 f 在 F' 上的分裂域．则伽罗瓦群 $G(K'/F')$ 同构于 G.

这一命题是个关键．它告诉我们如果 f 的伽罗瓦群为非阿贝尔单群，则如果用 F 的一个阿贝尔扩域 F' 代替 F，那么求它的根不会取得任何进展.

命题(9.8)的证明 我们首先化为 $[F':F]$ 为素数的情形．为此，假定命题对这一情形已证明，选择 $G(F'/F)$ 的一个素数阶循环商群 H．因为 $G(F'/F)$ 是阿贝尔群，所以这样的商是存在的．这个商确定一个中间域 $F_1 \subset F'$，它是 F 的伽罗瓦扩域，并且 $G(F_1/F)=H(5.7)$．设 K_1 是 f 在 F_1 上的分裂域．则由于 $[F_1:F]$ 为素数，$G(K_1/F_1)=G$．这样可以用 F_1 代替 F 而用 K_1 代替 K．对 $[F':F]$ 作归纳就可完成证明.

因此可以假定 $[F':F]=p$ 且 $H=G(F'/F)$ 是一个 p 阶循环群．分裂域 K' 包含一个 f 在 F 上的分裂域，称之为 K．于是我们归结为命题(9.7)的情形．因而 K' 在 F 上的伽罗瓦群 $\mathcal{G}$ 是 $G\times H$ 的子群，且它有到 G 的满映射．从而 $|G|$ 整除 $|\mathcal{G}|$，并且有 $|\mathcal{G}|$ 整除 $|G\times H|=p|G|$．如果 $|G|=|\mathcal{G}|$，则比较次数得 $K'=K$．在此情形，K 含有伽罗瓦扩域 F'，因此 H 是 G 的商群(5.7b)．由于 G 是非阿贝尔单群，这是不可能的．剩下仅有的可能性是 $\mathcal{G}=G\times H$．在域链 $F\subset F'\subset K'$ 上应用主要定理，我们得到 $G(K'/F')=G$，正是所要求的. ■

【9.9】定理 伽罗瓦群为 S_5 或 A_5 的五次多项式 $f(x)$ 的根不能在 F 上用根式表出.

证明 设 K 是 f 的分裂域．如果 $G=S_5$，则 f 的判别式不是 F 中的平方．在这种情形，我们用 $F(\delta)$ 代替 F，其中 δ 是 K 中判别式的平方根．伽罗瓦群 $G(K/F(\delta))$ 为 A_5．显然，只要证明 f 的根不能在较大的域上用根式表出即可．这就将群为 S_5 的情形化为了群为 A_5 的情形.

假设 f 在 F 上的伽罗瓦群为 A_5，但 f 的某个根 α 可在 F 上用根式表出．设 $\alpha\in F_r$，其中 F_r 是扩域链 $F=F_0\subset\cdots\subset F_r$ 的最后一项，链中每个扩域都是有循环伽罗瓦群的伽罗瓦扩域．由于 f 在 F 上的伽罗瓦群为单群，命题(9.8)归纳地指出对每个 i，f 在 F_i 上的伽罗瓦群也是 A_5．另一方面，由于它在 F_r 中有一个根 α，在这个域上 f 不再既约．因而 f 在 F_r 上的伽罗瓦群在 f 的一个分裂域中的五个根上的作用不是可迁的．特别地，伽罗瓦群不能是交错群．这是一个矛盾，它表明 f 的根不能在 F 上用根式表出. ■

573

我们现在将给出 $\mathbb{Q}$ 上的一个伽罗瓦群是 S_5 的特殊的五次多项式．5 是素数和伽罗瓦群在根 $\{\alpha_1,\cdots,\alpha_5\}$ 上可迁地作用这些事实极大地限制了可能的伽罗瓦群．例如，由于作用是可迁的，$|G|$ 能被 5 整除．这样 G 包含一个 5 阶元素．S_5 中仅有的 5 阶元素是如同 $\sigma=(\mathbf{12345})$ 的循环置换.

【9.10】引理 如果 G 中含有一个对换，则 $G=S_5$.

证明 如通常一样，对换 τ 是指交换两个指标的置换．我们可以假设 G 含有一个如上的循环置换 σ．必要时重新标号，可设 τ 作用为 $(\mathbf{1i})$．用 σ^{i-1} 代替 σ 并重新标号，化为 τ 是对换 $(\mathbf{12})$ 的情形．只需验证 σ 和 τ 生成 S_5，我们把它留作练习. ■

【9.11】推论 假设既约多项式(9.1)的根为 $\{\alpha_1,\cdots,\alpha_5\}$，并设 K 是它的分裂域．如果 $F(\alpha_1,\alpha_2,\alpha_3)<K$，则 $G(K/F)$ 是对称群 S_5.

因为设 $F'=F(\alpha_1,\alpha_2,\alpha_3)$．使得 $\alpha_1,\alpha_2,\alpha_3$ 不变的置换仅有 $(\mathbf{45})$．如果 $F'\neq K$，则这个置换必属于 $G(K/F')$．这样 $G(K/F)$ 中含有一个对换.

【9.12】推论　设 $f(x)$ 是$\mathbb{Q}$上一个恰有三个实根的五次既约多项式. 则它的伽罗瓦群是对称群, 因此它的根不能用根式表出.

因为若将实根记作 α_1, α_2, α_3. 则$\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)\subset\mathbb{R}$, 但由于 α_4, α_5 不是实的, K 不是$\mathbb{R}$的子域. 因而可以应用推论(9.11)得到 f 的伽罗瓦群是 S_5. 由定理(9.9), f 的根不能用根式表出.

【9.13】例　多项式 $x^5-16x=x(x^2-4)(x^2+4)$ 有三个实根, 但它当然不是既约的. 但我们可以加上一个小常数而不改变实根的个数. 这可通过观察多项式的图看出. 例如,

$$x^5-16x+2$$

仍有三个实根, 由艾森斯坦因准则[第十一章(4.5)], 它是既约的. 因而它的根不能在$\mathbb{Q}$上用根式表出.

我们提出的解后来没有推出任何结果.

Evariste Galois

574

练　习

第一节　伽罗瓦理论的主要定理

1. 在$\mathbb{Q}$上求 $i+\sqrt{2}$的既约多项式.
2. 证明集合$(1, i, \sqrt{2}, i\sqrt{2})$是$\mathbb{Q}(i, \sqrt{2})$在$\mathbb{Q}$上的一个基.
3. 求$\mathbb{Q}$与$\mathbb{Q}(\sqrt{2}, \sqrt{3})$间的中间域.
4. 不用主要定理求任意双二次扩域的中间域.
5. 证明将$\sqrt{2}$映到$-\sqrt{2}$的自同构是不连续的.
6. 求下列多项式在$\mathbb{Q}$上的分裂域的次数.
   (a) x^4-1　(b) x^3-2　(c) x^4+1
7. 用 α 表示 2 的实四次根. 在下面每个域上把多项式 x^4-2 分解成既约因子乘积: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha, i)$.
8. 设 $\zeta=e^{2\pi i/5}$.
   (a) 证明 $K=\mathbb{Q}(\zeta)$是多项式 x^5-1 在$\mathbb{Q}$上的分裂域, 并求次数$[K:\mathbb{Q}]$.
   (b) 不用定理(1.11), 证明 K 是$\mathbb{Q}$上的伽罗瓦扩域, 并求其伽罗瓦群.
9. 设 K 是形如 $F(\alpha)$的二次扩域, 其中 $\alpha^2=a\in F$. 求 K 中所有平方属于 F 的元素.
10. 设 $K=\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. 求$[K:\mathbb{Q}]$, 证明 K 是$\mathbb{Q}$上的伽罗瓦扩域, 并求其伽罗瓦群.
11. 设 K 是多项式 $f(x)=(x^2-2x-1)(x^2-2x-7)$在$\mathbb{Q}$上的分裂域. 求 $G(K/\mathbb{Q})$, 并具体求出所有中间域.
12. 求域$\mathbb{Q}(\sqrt[3]{2})$的所有自同构.
13. 设 K/F 是个有限扩域. 证明伽罗瓦群 $G(K/F)$是有限群.
14. 对一个素数 $p\neq2$, 求含有一个 p 次本原单位根的所有二次数域$\mathbb{Q}[\sqrt{d}]$.
15. 证明其伽罗瓦群为克莱因四元群的每个伽罗瓦扩域 K/F 是双二次的.
16. 证明或推翻: 设 $f(x)$是$\mathbb{Q}[x]$中有一个实根 α 的三次既约多项式. 它的另外的根构成复共轭对 β, $\bar{\beta}$, 因而域 $L=\mathbb{Q}(\beta)$有一个使 β, $\bar{\beta}$ 交换的自同构 σ.

17. 设K是域F的伽罗瓦扩域，且使得$G(K/F)\approx C_2\times C_{12}$. 有多少个中间域$L$使得(a)$[L:F]=4$, (b)$[L:F]=9$,(c)$G(K/L)\approx C_4$?
18. 设$f(x)=x^4+bx^2+c\in F[x]$，并设K是f的分裂域. 证明$G(K/F)$包含在二面体群D_4之中.
19. 设$F=\mathbb{F}_2(u)$是二元域上的有理函数域. 证明多项式x^2-u在$F[x]$中既约并且它在分裂域中有两个相等的根.
20. 设F是特征为2的域，并设K是F上的二次扩域.
    (a) 证明K具有$F(\alpha)$的形式，其中α是F上形如x^2+x+a的既约多项式的根，这个方程的另一个根是$\alpha+1$.
    (b) 是否存在K的自同构使$\alpha \rightsquigarrow \alpha+1$?

575

第二节 三次方程

1. 证明如果实三次多项式的所有根皆是实根，则判别式为正，否则判别式为负.
2. 求下列多项式的伽罗瓦群.
   (a) x^3-2 (b) $x^3+27x-4$ (c) x^3+x+1 (d) $x^3+3x+14$
   (e) x^3-3x^2+1 (f) $x^3-21x+7$ (g) x^3+x^2-2x-1 (h) x^3+x^2-2x+1
3. 设f是F上的三次既约多项式，并设δ是f的判别式的平方根. 证明f在域$F(\delta)$上仍是既约的.
4. 设α是$\mathbb{Q}$上多项式x^3+x+1的复根，并设K是这个多项式在$\mathbb{Q}$上的分裂域.
   (a) $\sqrt{-3}$属于$\mathbb{Q}(\alpha)$吗? 属于K吗?
   (b) 证明域$\mathbb{Q}(\alpha)$除了恒等映射外没有其他自同构.
*5. 对形如(2.3)的三次多项式，通过具体求出将α_2用α_1，δ，p，q表出的公式直接证明命题(2.16).
6. 设$f(x)\in\mathbb{Q}[x]$为一个恰有一个实根的三次既约多项式，并设K是它在$\mathbb{Q}$上的分裂域. 证明$[K:\mathbb{Q}]=6$.
7. 什么时候多项式x^3+px+q有重根?
8. 对一般三次多项式，求(2.1)作代入(2.2)后得到的系数p，q.
9. 证明三次多项式x^3+px+q的判别式为$-4p^3-27q^2$.

第三节 对称函数

1. 用待定系数法推导出三次多项式的判别式的表达式(3.10).
2. 设$f(u)$是u_1，…，u_n的d次对称多项式，并设$f^0(u_1,\cdots,u_{n-1})=f(u_1,\cdots,u_{n-1},0)$. 假定$f^0(u)=g(s^0)$,其中$s_i^0$是$u_1$，…，$u_{n-1}$的初等对称函数. 证明如果$n>d$，则$f(u)=g(s)$.
3. 计算形如x^5+ax+b的五次多项式的判别式.
4. 对下面每个多项式，确定它是否是对称函数，如果是的话，把它用初等对称函数表示出来.
   (a) $u_1^2u_2+u_2^2u_1(n=2)$
   (b) $u_1^2u_2+u_2^2u_3+u_3^2u_1(n=3)$
   (c) $(u_1+u_2)(u_2+u_3)(u_1+u_3)(n=3)$
   (d) $u_1^3u_2+u_2^3u_3+u_3^3u_1-u_1u_2^3-u_2u_3^3-u_3u_1^3(n=3)$
   (e) $u_1^3+u_2^3+\cdots+u_n^3$
5. 求对称函数环作为环R上自由模的两个自然的基.

576

*6. 用$w_k=u_1^k+\cdots+u_n^k$定义变量u_1，…，u_n的多项式w_1，…，w_n.
   (a) 证明牛顿恒等式：$w_k-s_1w_{k-1}+s_2w_{k-2}-\cdots\pm s_{k-1}w_1\mp ks_k=0$.
   (b) w_1，…，w_n生成对称函数环吗?
7. 设$f(x)=x^3+a_2x^2+a_1x+a_0$. 证明代入$x=x_1-(a_2/3)$并不改变三次多项式的判别式.
8. 直接由定义用归纳法证明$[F(u):F(s)]=n!$.

9. 设 u_1，…，u_n 是变量并用 D_1 表示判别式．定义

$$D_2 = \sum_k \prod_{\substack{i<j \\ i,j\neq k}} (u_i - u_j)^2.$$

(a) 证明 D_2 是对称多项式，并对 $n=2$，3 的情形计算它用初等对称多项式表出的表达式．

(b) 设 a_1，…，a_n 是特征为零的域中的元素．证明 $D_1(a_1, \cdots, a_n)=D_2(a_1, \cdots, a_n)=0$ 当且仅当集合 $\{a_1, \cdots, a_n\}$ 中不同元素的个数 $\leqslant n-2$．

10. 计算第二节练习 2 给出的多项式的判别式．

*11. （范德蒙德行列式）(a) 证明矩阵

$$\begin{bmatrix} 1 & u_1 & u_1^2 & \cdots & u_1^{n-1} \\ 1 & u_2 & & & u_2^{n-1} \\ \vdots & & & & \\ 1 & u_n & u_n^2 & \cdots & u_n^{n-1} \end{bmatrix}$$

是 $\delta(u)$ 的常数倍．

(b) 确定这个常数．

第四节　本原元

1. 设 G 是域 K 的自同构群．证明不变元集合 K^G 构成 K 的子域．

2. 设 $\alpha=\sqrt[3]{2}$，$\zeta=\frac{1}{2}(-1+\sqrt{-3})$，$\beta=\alpha\zeta$．

(a) 证明对所有 $c\in\mathbb{Q}$，$\gamma=\alpha+c\beta$ 是形如 x^6+ax^3+b 的六次多项式的根．

(b) 证明 $\alpha+\beta$ 的既约多项式是三次的．

(c) 证明 $\alpha-\beta$ 在 $\mathbb{Q}$ 上的次数为 6．

3. 对下面的有理函数域 $\mathbb{C}(y)$ 的自同构集中的每一个，确定它们生成的每一个自同构群，并具体确定其不变域．

(a) $\sigma(y)=y^{-1}$　(b) $\sigma(y)=\mathrm{i}y$　(c) $\sigma(y)=-y$，$\tau(y)=y^{-1}$　(d) $\sigma(y)=\zeta y$，$\tau(y)=y^{-1}$，其中 $\zeta=e^{2\pi i/3}$

(e) $\sigma(y)=\mathrm{i}y$，$\tau(y)=y^{-1}$

4. (a) 证明 $\mathbb{C}(y)$ 的自同构 $\sigma(y)=(y+\mathrm{i})/(y-\mathrm{i})$，$\tau(y)=\mathrm{i}(y-1)/(y+1)$ 生成一个与交错群 A_4 同构的群．

*(b) 确定这个群的不变域．

577 *5. 设 F 是有限域，并设 $f(x)$ 是其导数为零多项式的非常数多项式．证明 f 在 F 上不是既约的．

第五节　主要定理的证明

1. 设 $K=\mathbb{Q}(\alpha)$，其中 α 是多项式 x^3+2x+1 的根，且设 $g(x)=x^3+x+1$．$g(x)$ 在 K 中有根吗？

2. 设 $f\in F[x]$ 是一个 n 次多项式，并设 K 是 f 的分裂域．证明 $[K:F]$ 整除 $n!$．

3. 设 G 是个有限群．证明存在一个域 F 及 F 的一个伽罗瓦扩域 K，其伽罗瓦群为 G．

4. 假设已知 π 和 e 是超越数．设 K 是多项式 $x^3+\pi x+6$ 在域 $F=\mathbb{Q}(\pi)$ 上的分裂域．

(a) 证明 $[K:F]=6$．

(b) 证明 K 同构于多项式 x^3+ex+6 在 $\mathbb{Q}(e)$ 上的分裂域．

5. 使用商构造的泛性形式地证明引理(5.1)的证明中使用的同构 $F[x]/(f(x))\approx\widetilde{F}[x]/(\widetilde{f}(x))$．

6. 证明推论(5.5)．

7. 设 $f(x)$ 是在 $\mathbb{Q}$ 上伽罗瓦群为 S_3 的三次既约多项式．求多项式 $(x^3-1)\cdot f(x)$ 可能的伽罗瓦群．

8. 考虑域的图 $\begin{array}{ccc} & K' & \\ \cup & & \cup \\ K & & F' \\ \cup & & \cup \\ & F & \end{array}$，其中 K 是 F 的伽罗瓦扩域，而 K' 在 F 上由 K 和 F' 生成．证明 K' 是 F' 的伽罗瓦扩域，且其伽罗瓦群同构于 $G(K/F)$ 的一个子群．

9. 设 $K\supset L\supset F$ 是域. 证明或推翻：
   (a) 如果 K/F 是伽罗瓦的，则 K/L 是伽罗瓦的.
   (b) 如果 K/F 是伽罗瓦的，则 L/F 是伽罗瓦的.
   (c) 如果 L/F 和 K/L 是伽罗瓦的，则 K/F 是伽罗瓦的.
10. 设 K 是三次既约多项式 $f(x)$ 在域 F 上的分裂域，其伽罗瓦群为 S_3. 求扩域 $F(\alpha)$ 的自同构群 $G(F(\alpha)/F)$.
11. 设 K/F 是伽罗瓦群为对称群 S_3 的伽罗瓦扩域. K 是否是 F 上三次既约多项式的分裂域？
12. 设 K/F 是一个特征 $p\neq 0$ 的扩域，并设 α 是 F 上既约多项式 $f(x)=x^p-x-a$ 在 K 中的根.
   (a) 证明 $\alpha+1$ 也是 $f(x)$ 的根.
   (b) 证明 f 在 F 上的伽罗瓦群是 p 阶循环群.

第六节　四次方程

1. 计算四次多项式 x^4+1 的判别式，并确定它在$\mathbb{Q}$上的伽罗瓦群.
2. 设 K 是一个四次既约多项式 $f(x)$ 在 F 上的分裂域，并设 $f(x)$ 在 K 中的根为 α_1，α_2，α_3，α_4. 再假设其三次预解式 $g(x)$ 有一个根，设为 $\beta_1=\alpha_1\alpha_2+\alpha_3\alpha_4$. 把根 α_1 用一系列平方根具体表出.
3. 对于恰好有两个实根的$\mathbb{Q}$上的四次既约多项式的伽罗瓦群你有什么结论？
4. 假设实四次多项式有正的判别式. 对于其实根的个数你有什么结论？
5. 设 K 是在 F 上有不同根的可约的四次多项式的分裂域. K/F 可能的伽罗瓦群是什么？
6. $\mathbb{Q}$上判别式为负的四次既约多项式可能的伽罗瓦群是什么？
7. 设 g 是四次既约多项式 $f\in F[x]$ 的三次预解式. 求 g 在 F 上可能的伽罗瓦群，并在每一种情形，给出关于 f 的伽罗瓦群的可能结论.
8. 设 K 是有互不相同的根 α_1，…，α_n 的多项式 $f\in F[x]$ 的分裂域，并设 $G=G(K/F)$. 则 G 可以视为对称群 S_n 的子群. 证明根的指标变化将群 G 变为一个共轭子群.
9. 设 α_1，…，α_4 是四次多项式的根. 按书中讨论的思路讨论 $\alpha_1\alpha_2$ 和 $\alpha_1+\alpha_2$ 的对称.
10. 求$\mathbb{Q}$上伽罗瓦群为(a)S_4，(b)D_4，(c)C_4 的四次多项式.
11. 设 α 是$\mathbb{Q}$上四次多项式 f 的实根. 假设其三次预解式是既约的. 证明 α 不能用直尺和圆规作出.
12. 求下列多项式在$\mathbb{Q}$上的伽罗瓦群.
   (a) x^4+4x^2+2　(b) x^4+2x^2+4　(c) x^4+4x^2-5　(d) x^4-2　(e) x^4+2　(f) x^4+1　(g) x^4+x+1
   (h) $x^4+x^3+x^2+x+1$　(i) x^4+x^2+4
13. 用引理(8.7)的公式计算四次多项式 x^4+ax+b 的判别式.
*14. 设 f 是 F 上一个形如 x^4+rx+s 的四次既约多项式，并设 α_1，α_2，α_3，α_4 是 f 在一个分裂域 K 中的根. 设 $\eta=\alpha_1\alpha_2$.
   (a) 证明 η 是系数属于 F 的六次多项式 $h(x)$ 的根.
   (b) 假设六个积 $\alpha_i\alpha_j$ 互不相同，证明 $h(x)$ 或是既约的，或者它有一个既约的二次因子.
   (c) 对下列三种情形描述可能的伽罗瓦群 $G=G(K/F)$：h 既约；h 是一个既约二次多项式和一个既约四次多项式的乘积；h 是三个既约二次多项式的乘积.
   (d) 描述某些积相等的情形.
15. 设 K 是$\mathbb{Q}$上多项式 x^4-3 的分裂域.
   (a) 证明$[K:\mathbb{Q}]=8$ 且 K 由 i 和多项式的单独一个根 α 生成.
   (b) 证明 $K/\mathbb{Q}$ 的伽罗瓦群是二面体群，并具体描述 G 的元素在 K 的生成元上的作用.
16. 设 K 是多项式 x^4-2x^2-1 在$\mathbb{Q}$上的分裂域. 求 $K/\mathbb{Q}$ 的伽罗瓦群 G，求出所有的中间域，并将它们与 G 的子群配对.

578

579

17. 设 $f(x)$是四次多项式. 证明 f 的判别式与它的三次预解式相等.
18. 证明多项式(6.17)和它的三次预解式的既约性.
19. 设 K 是可约多项式$(x-1)^2(x^2+1)$在$\mathbb{Q}$上的分裂域. 证明$\delta\in\mathbb{Q}$，但$G(K/\mathbb{Q})$不含于交错群中.
20. 设 $f(x)$是根互不相同的四次多项式，其三次预解式 $g(x)$在 F 中完全分裂. $f(x)$可能的伽罗瓦群是什么？
21. 设 $\zeta=e^{2\pi i}/3$ 是 1 的立方根，设 $\alpha=\sqrt[3]{a+b\sqrt{2}}$，并设 K 是 α 的既约多项式在$\mathbb{Q}(\zeta)$上的分裂域. 确定 K 在$\mathbb{Q}(\zeta)$上可能的伽罗瓦群.
22. 设$\mathcal{H}$是对称群 S_n 的子群. 给定任意单项式 m，我们可构造多项式 $p(u)=\sum_{\sigma\in\mathcal{H}}\sigma m$. 证明如果 $m=u_1u_2^2u_3^3\cdots u_{n-1}^{n-1}$，则 $p(u)$ 关于$\mathcal{H}$是部分对称的；即它在$\mathcal{H}$的每个置换下不变，但在任意其他置换下都不是不变的.
23. 设 $p(u)$是上一个问题中构造的多项式，其中$\mathcal{H}=A_n$. 则 $p(u)$的轨道含有两个元素，设为 $p(u)$，$q(u)$. 证明 $p(u)-q(u)=\pm\delta(u)$.
24. 假定二次多项式 y^2+by+c 既约，确定形如 x^4+bx^2+c 的可约四次多项式可能的伽罗瓦群.
25. 通过对 x^4-x 和 x^4-1 取值计算 x^4+rx+s 的判别式.
26. 用代入 $x\rightsquigarrow y^{-1}$求多项式 x^4+ax^3+b 的判别式.
27. 求多项式(a)x^4+rx+s 和(b)$x^4+a_1x^3+a_2x^2+a_3x+a_4$ 的三次预解式.
28. 设 $f(x)=x^4-2rx^2+(r^2-s^2v)$，其中 r，s，$v\in F$. 假定 f 既约，并且设 G 表示其伽罗瓦群. 设 $L=F(\sqrt{v},\delta)$，其中 $\delta^2=D$. 证明下面的每个断言.
    (a) $L(\alpha)=K$.
    (b) 如果$[L:F]=4$，则 $G=D_4$.
    (c) 如果$[L:F]=2$ 且 $\delta\notin F$，则 $G=C_4$.
29. 求(6.5)最后两个例子的伽罗瓦群.
30. 假定(a)$G=C_4$，(b)$G=D_4$，具体确定伽罗瓦群 G 在根$\{\alpha,\alpha',-\alpha,-\alpha'\}$(6.7)上的作用.
31. 确定下列嵌套根式是否可以用非嵌套根式写出，如果可以，写出表达式.
    (a) $\sqrt{2+\sqrt{11}}$　(b) $\sqrt{6+\sqrt{11}}$　(c) $\sqrt{11+6\sqrt{2}}$　(d) $\sqrt{11+\sqrt{6}}$
*32. 设 K 是$\mathbb{Q}$上伽罗瓦群为 D_4 的四次多项式 $f(x)$的分裂域，并设 α 是 f 在 K 中的一个实根. 如果(a)f 的四个根全是实根，(b)f 有两个实根，确定 α 是否能用直尺和圆规作出.
33. 多项式 x^4+x-5 的根能用直尺和圆规作出吗？

第七节 库默尔扩域

1. 假定伽罗瓦扩域 K/F 具有 $K=F(\alpha)$的形式，且对某个整数 n 有 $\alpha^n\in F$. 关于 K/F 的伽罗瓦群你有什么结论？

580

*2. 设 a 是域 F 的元素，并设 p 是一个素数. 假设 x^p-a 在 $F[x]$中可约. 证明它在 F 中有一个根.
3. 设 F 是$\mathbb{C}$的一个包含 i 的子域，并设 K 是 F 上群为 C_4 的伽罗瓦扩域. K 是否有 $F(\alpha)$的形式，其中 $\alpha^4\in F$?
4. 设 $f(x)=x^3+px+q$ 是域 F 上的既约多项式，其根为 α_1，α_2，α_3. 令 $\beta=\alpha_1+\zeta\alpha_2+\zeta^2\alpha_3$，其中 $\zeta=e^{2\pi i/3}$. 证明只要 $\beta\neq0$，则 β 是根的循环置换 σ 的一个特征根，并用 p，q，δ，ζ 具体计算 β^3.
5. 设 K 是 p 次既约多项式 $f(x)\in F[x]$的分裂域，其伽罗瓦群是由 σ 生成的 p 阶循环群，并假设 F 含有 p 次单位根 $\zeta=\zeta_p$. 设 α_1，…，α_p 是 f 在 K 中的根. 证明 $\beta=\alpha_1+\zeta^v\alpha_2+\zeta^{2v}\alpha_3+\cdots+\zeta^{(p-1)v}\alpha_p$ 只要不等于零，就是 σ 的一个特征值为 ζ^{-v}的特征向量.
6. 设 $f(x)=x^3+px+q$ 是复数的子域 F 上的既约多项式，复根为 $\alpha=\alpha_1$，α_2，α_3. 令 $K=f(\alpha)$.
    (a) 将$(6\alpha^2+2p)^{-1}$具体表示为 α 的二次多项式.

(b) 假定 $\delta=\sqrt{D}$属于 F，因而 K 含有 f 的其他根. 将 α_2 表示为 $\alpha=\alpha_1$ 和 δ 的多项式.

(c) 证明$(1, \alpha_1, \alpha_2)$是 K 作为 F-向量空间的一个基.

(d) 设 φ 是循环地置换三个根的 K 的自同构. 写出 φ 关于上面这个基的矩阵，并求它的特征值和特征向量.

(e) 设 v 是一个特征值为 $\zeta=e^{2\pi i/3}$ 的特征向量. 证明如果 $\sqrt{-3}\in F$，则 $v^3\in F$. 用 p，q，δ，$\sqrt{-3}$具体算出 v^3.

(f) 去掉 δ 和 $\sqrt{-3}$属于 F 的假设，将 v 用根式表出.

(g) 不用计算，确定由交换 α_1，α_2 的角色从 v 得到的元素 v'.

(h) 将根 α_1 用根式表达出来.

第八节　分圆扩域

1. 求域$\mathbb{Q}(\zeta_3)$上 ζ_7 的次数.
2. 设 $\zeta=\zeta_{13}$，并设 $K=\mathbb{Q}(\zeta)$. 具体求出$\mathbb{Q}$上的三次中间域.
3. 设 $\zeta=\zeta_{17}$. 具体求出生成域$\mathbb{Q}(\zeta+\zeta^{16})$的平方根系列.
4. 设 $\zeta=\zeta_7$. 求下列元素在$\mathbb{Q}$上的次数.

   (a) $\zeta+\zeta^5$　(b) $\zeta^3+\zeta^4$　(c) $\zeta^3+\zeta^5+\zeta^6$
5. 设 $\zeta=\zeta_{13}$. 求下列元素在$\mathbb{Q}$上的次数.

   (a) $\zeta+\zeta^{12}$　(b) $\zeta+\zeta^2$　(c) $\zeta+\zeta^5+\zeta^8$　(d) $\zeta^2+\zeta^5+\zeta^6$　(e) $\zeta+\zeta^5+\zeta^8+\zeta^{12}$　(f) $\zeta+\zeta^2+\zeta^5+\zeta^{12}$

   (g) $\zeta+\zeta^3+\zeta^4+\zeta^9+\zeta^{10}+\zeta^{12}$
6. 设 $\zeta=\zeta_{11}$.

   (a) 证明 $\alpha=\zeta+\zeta^3+\zeta^4+\zeta^5+\zeta^9$ 在$\mathbb{Q}$上生成一个次数为 2 的域，并求它的多项式.

   (b) 求一个在$\mathbb{Q}$上生成一个 5 次子域的元素，并求它的多项式.
7. 证明$\mathbb{Q}$上每个二次扩域包含在一个分圆扩域中.
8. 设 $K=\mathbb{Q}(\zeta_n)$.

   (a) 证明 K 是$\mathbb{Q}$的伽罗瓦扩域.

   (b) 定义到环$\mathbb{Z}/(n)$的单位元群 U 的单同态 v：$G(K/\mathbb{Q})\longrightarrow U$.

   (c) 证明当 $n=6$，8，12 时，这个同态是一一的(实际上，这个映射总是一一的.)

*9. 设 p 是素数，并设 a 是一个不是 p 次幂的有理数. 设 K 是多项式 x^p-a 在$\mathbb{Q}$上的分裂域.

   (a) 证明 K 由 a 的一个 p 次根 α 及一个 p 次本原单位根 ζ 在$\mathbb{Q}$上生成.

   (b) 证明$[K:\mathbb{Q}]=p(p-1)$.

   (c) 证明 $K/\mathbb{Q}$ 的伽罗瓦群同构于形如$\begin{bmatrix}a & b\\ & 1\end{bmatrix}$的元素属于$\mathbb{F}_p$ 的可逆 2×2 矩阵的群. 具体描述$\begin{bmatrix}a & \\ & 1\end{bmatrix}$和$\begin{bmatrix}1 & b\\ & 1\end{bmatrix}$在生成元上的作用.

10. 求多项式 x^8-1，$x^{12}-1$，x^9-1 的伽罗瓦群.
11. (a) 刻画使正 p 边形可用直尺和圆规作出的素数 p.

    (b) 将刻画拓广到正 n 边形的情形，其中 n 不必是素数.

*12. 设 v 是模素数 p 的本原元，并设 d 是 $p-1$ 的一个因数. 说明如何用单位根的列表$\{\zeta, \zeta^v, \zeta^{v^2}, \cdots, \zeta^{v^{p-2}}\}$确定 $\zeta=\zeta_p$ 的幂的和，使它生成$\mathbb{Q}$上次数为 d 的$\mathbb{Q}(\zeta)$的子域 L.

第九节　五次方程

1. 确定 S_5 的可迁子群.
2. 设 G 是五次既约多项式的伽罗瓦群. 证明如果 G 包含一个 3 阶元，则 $G=S_5$ 或 A_5.

581

*3. 设 p 是一个素整数，并设 G 是一个 p-群. 设 H 是 G 的一个真正规子群.

(a) 证明 H 的正规化子 $N(H)$ 严格大于 H.

(b) 证明 H 含于一个指标为 p 的子群中并且这个子群在 G 中正规.

(c) 设 K 是$\mathbb{Q}$上次数为 2 的幂的伽罗瓦扩域，并且 $K\subset\mathbb{R}$. 证明 K 的元素可用直尺和圆规作出.

4. 设 $K\supset L\supset F$ 是二次域的扩域塔. 证明 K 可以由形如 x^4+bx^2+c 的四次既约多项式的根在 F 上生成.

*5. 卡尔达诺公式有一个特别的性质：假设三次多项式的系数 p, q 为实数. 一个实三次多项式总有至少一个实根. 然而，如果$(q/2)^2+(p/3)^3<0$，则公式(2.6)中出现的平方根将是虚的. 这时，实根可用一个辅助的复数 u 表出. 在卡尔达诺时代这被认为是不合适的. 设 $f(x)$是$\mathbb{R}$的一个子域 F 上的有三个实根的既约三次多项式. 证明 f 的根不能用实根式表出，也就是说不存在如(9.2)那样的根塔 $F=F_0\subset\cdots\subset F_r$，使得其中所有域都是$\mathbb{R}$的子域.

582

6. 设 $f(x)\in F[x]$是五次既约多项式，并设 K 是 $f(x)$在 F 上的分裂域.

(a) 假定判别式 D 是 F 中的一个平方数，可能的伽罗瓦群 $G(K/F)$是什么.

*(b) 如果 D 不是 F 中的一个平方数，可能的伽罗瓦群是什么?

7. 用其对应多项式的伽罗瓦群确定$\mathbb{Q}$上哪些四次实数 α 可以用直尺和圆规作出.

8. 是否每一个十次伽罗瓦扩域都能用根式求解?

*9. 求一个$\mathbb{Q}$上伽罗瓦群为 S_7 的七次多项式.

杂题

1. 设 K 是 F 上伽罗瓦群为对称群 S_4 的伽罗瓦扩域. K 的元素在 F 上的次数会是些什么数?

2. 不用计算证明单位元内接正五边形的边长在$\mathbb{Q}$上次数为 2.

3. (a) 非负实数是有实平方根的实数. 用这个事实证明域$\mathbb{R}$除了恒等映射外没有其他自同构.

(b) 证明除了复共轭和恒等映射外$\mathbb{C}$没有其他连续自同构.

4. 设 K/F 是伽罗瓦群为 G 的伽罗瓦扩域，并设 H 是 G 的子群. 证明存在一个稳定子为 H 的元素 $\beta\in K$.

*5. (a) 设 K 是特征为 p 的域. 证明由 $\varphi(x)=x^p$ 定义的弗洛贝尼乌斯映射 φ 是 K 到自身的同态.

(b) 证明如果 K 是有限域，则 φ 是个同构.

(c) 举出一个使 φ 不是同构的特征 p 的无限域的例子.

(d) 设 $K=\mathbb{F}_q$，其中 $q=p^r$，并设 $F=\mathbb{F}_p$. 证明 $G(K/F)$是由弗洛贝尼乌斯映射 φ 生成的 r 阶循环群.

(e) 证明对扩域 K/F，伽罗瓦理论的主要定理成立.

6. 设 K 是$\mathbb{C}$的子域，并设 G 是其自同构群. 我们可以视 G 在复平面上的点集 K 上作用. 作用可能是不连续的，然而，我们可通过定义 $g[\alpha, \beta]=[g\alpha, g\beta]$来定义一个在端点属于 K 的线段$[\alpha, \beta]$上的作用. 于是 G 也作用在顶点属于 K 的多边形之上.

(a) 设 $K=\mathbb{Q}(\zeta)$，其中 ζ 是五次本原单位根. 求顶点为 1, ζ, ζ^2, ζ^3, ζ^4 的正五边形的 G-轨道.

(b) 设 α 是(a)中五边形的边长. 证明 $a=\alpha^2\in K$，并求 α 在$\mathbb{Q}$上的既约方程. $\alpha\in K$ 吗?

7. 一个多项式 $f\in F[x_1, \cdots, x_n]$称为 $\frac{1}{2}$-对称的，如果对每个下标的偶置换 σ 有 $f(u_{\sigma 1}, \cdots, u_{\sigma n})=f(u_1, \cdots, u_n)$，而称为斜对称的，如果对每个置换 σ 有 $f(u_{\sigma 1}, \cdots, u_{\sigma n})=(\operatorname{sign}\sigma)f(u_1, \cdots, u_n)$.

(a) 证明判别式的平方根 $\delta=\prod\limits_{i<j}(u_i-u_j)$ 是斜对称的.

(b) 证明每个$\frac{1}{2}$-对称多项式具有 $f+g\delta$ 的形式，其中 f, g 是对称多项式.

*8. 设 $f(x, y)\in\mathbb{C}[x, y]$是一个既约多项式，我们将其视为 y 的多项式 $f(y)$. 假设 f 作为 y 的多项式是三次的. 它关于变量 y 的判别式 D 是一个 x 的多项式. 假定 $D(x)$有一个不是重根的根 x_0.

583

(a) 证明 y 的多项式 $f(x_0, y)$有一个单根和一个重根.

(b) 证明 $f(y)$在$\mathbb{C}[x]$上的分裂域 K 的次数为 6.

9. 设 K 是$\mathbb{C}$的子域且是$\mathbb{Q}$的伽罗瓦扩域. 证明或推翻：复共轭将 K 变到自身，因而它定义 K 上的一个自同构.

*10. 设 K 是域 F 的有限扩域，并设 $f(x)\in K[x]$. 证明存在非零多项式 $g(x)\in K[x]$使得 $f(x)g(x)\in F[x]$.

*11. 设 $f(x)$是 $F[x]$中的四次既约多项式. 设 α_1，α_2，α_3，α_4 是它在分裂域 K 中的根. 假设三次预解式在 F 中有一个根 $\beta=\alpha_1\alpha_2+\alpha_3\alpha_4$，但判别式 D 不是 F 中的平方数. 根据书中所述，K/F 的伽罗瓦群是 C_4 或 D_4.

(a) 具体求出稳定 β 的根 α_i 的置换群 S_4 的子群 H. 不要忘记证明除了你列出的置换外，其他置换都不能使 β 不变.

(b) 设 $\gamma=\alpha_1\alpha_2-\alpha_3\alpha_4$ 而 $\varepsilon=\alpha_1+\alpha_2-\alpha_3-\alpha_4$. 描述 H 在这些元素上的作用.

(c) 证明 γ^2 和 ε^2 属于 F.

(d) 设 δ 是判别式的平方根. 证明如果 $\gamma\neq 0$，则 $\delta\gamma$ 是 F 中的平方数当且仅当 $G=C_4$. 同样地，证明如果 $\varepsilon\neq 0$，则 $\delta\varepsilon$ 是 F 中的平方数当且仅当 $G=C_4$.

(e) 证明 γ 和 ε 不能同时为零.

*12. 设 $F=\mathbb{F}_p(u, v)$为有 p 个元素的域$\mathbb{F}_p$ 上的两个变量的有理函数域，并设 $K=F(\alpha, \beta)$，其中 α，β 分别是多项式x^p-u和 x^p-v 的根. 证明下面的结论：

(a) 扩域 K/F 没有本原元.

(b) 元素 $\gamma=\beta+c\alpha$(其中 $c\in F$)生成无限多个互不相同的中间域 L.

*13. 设 K 是有 p^r 个元素的域. 当 K 视为素域 $F=\mathbb{F}_p$ 上的向量空间时，证明由 $\varphi(z)=z^p$ 定义的弗洛贝尼乌斯映射 φ 是 K 的线性变换，并求其特征向量和特征值.

584

这种方法能做到些什么，

只有将来才知道.

Emmy Noether

附录 背景材料

当然从历史上讲，没有矛盾的数学是相当不真实的；
没有矛盾是一个想要达到的目标，
而不是上帝赋予我们的一劳永逸的质量.

Emmy Bourbaki

第一节 集 合 论

本节复习本书所用到的集合论的约定以及我们经常用到的一些事实.

首先是一个关于定义的备注：一个术语或短语的任何定义大致上有这样的形式：

【1.1】 xxx 如果 #&$%，

其中 xxx 是定义的术语，而#&$%是其定义的性质. 例如，句子"一个整数 n 是正的，如果 $n>0$"定义一个正整数的概念. 在一个定义中，"如果"一词是指"当且仅当". 因而在正整数的定义中，所有不满足要求 $n>0$ 的整数都被排除在外.

记号

【1.2】 $\{s \in S \mid$ #&$% $\}$

是指 S 中使得#&$%成立的元素 s 的子集合. 这样如果$\mathbb{Z}$ 表示所有整数的集合，则$\mathbb{N}=\{n\in\mathbb{Z} \mid n>0\}$把$\mathbb{N}$ 描述为所有正整数或自然数的集合.

一个集合的元素 $a_1, \cdots, a_n$ 称为不同的，如果其中没有两个元素是相等的.

从集合 S 到集合 T 的一个映射是任一个定义域为 S 而值域是 T 的函数. 术语函数和映射作为同义词使用. 我们要求函数是单值的. 这是说每一个元素 $s\in S$ 必须有唯一确定的象 $\varphi(s)\in T$. φ 的值域 T 不要求是函数的值的集合. 由函数的定义，每一个象元素 $\varphi(s)$包含在 T 中，但允许某些元素 $t\in T$ 根本不被函数取到. 我们把函数的定义域和值域也作为其定义的一部分. 如果把定义域限制到一个子集合，或者拓广值域，则得到的函数被认为是不同的.

585

映射的定义域和值域也可以使用一个箭头描述. 这样记号 $\varphi: S\longrightarrow T$ 告诉我们 φ 是一个从 S 到 T 的映射. $t=\varphi(s)$这一断言可以用一个波尾箭头描述：$s \rightsquigarrow t$，这是指在所考虑的映射下元素$s\in S$ 被映到 $t\in T$. 例如，使 $\varphi(n)=2n+1$ 的映射 $\varphi:\mathbb{Z}\longrightarrow\mathbb{Z}$ 被描述为 $n \rightsquigarrow 2n+1$.

映射 φ 的象是 T 的对某个 $s\in S$ 具有形式 $\varphi(s)$的元素的子集合. 它常常记为 $\mathrm{im}\varphi$ 或 $\varphi(S)$：

【1.3】 $\mathrm{im}\varphi=\{t\in T \mid$ 对某个 $s\in S$ 有 $t=\varphi(s)\}$.

当 $\mathrm{im}\varphi$ 是整个值域 T 时，映射称为是满的. 从而 φ 是满射如果每个 $t\in T$ 具有 $\varphi(s)$的形状，其中 $s\in S$.

映射称为单的，如果 S 的不同元素 s_1，s_2 有不同的象，即如果 $s_1\neq s_2$ 蕴涵 $\varphi(s_1)\neq\varphi(s_2)$. 既是单的又是满的映射称为一一映射. 集合 S 的置换是从 S 到自身的一一映射.

设 $\varphi: S\longrightarrow T$ 和 ψ：$T\longrightarrow S$ 是两个映射. ψ 称为 φ 的逆函数，如果两个合成映射 $\varphi\circ\psi$：$T\to T$ 和 $\psi\circ\varphi$：$S\to S$ 都是恒等映射，即如果对所有 $t\in T$ 有 $\varphi(\psi(t))=t$ 而对所有 $s\in S$ 有

$\psi(\varphi(s))=s$. 逆函数通常记作 φ^{-1}.

【1.4】命题　映射 $\varphi:S\longrightarrow T$ 有逆函数当且仅当它是一一的.

证明　假设 φ 有逆函数 ψ，我们证明 φ 同时是满的和单的. 设 t 是 T 的任意元素，并设 $s=\psi(t)$. 则 $\varphi(s)=\varphi(\psi(t))=t$. 因而 t 属于 φ 的象. 这表明 φ 是满射. 其次，设 s_1，s_2 是 S 的不同元素，并设 $t_i=\varphi(s_i)$. 则 $\psi(t_i)=s_i$. 因而 t_1，t_2 在 S 中有不同的象，这表明它们是不同的元素. 因而 φ 是单射. 反过来，假设 φ 是一一的. 则由于 φ 是满的，每一个元素 $t\in T$ 具有 $t=\varphi(s)$ 的形式，其中 $s\in S$. 由于 φ 是单的，只能有一个这样的元素 s. 因而我们用下面的法则定义 ψ：$\psi(t)$ 是使得 $\psi(s)=t$ 的唯一元素 $s\in S$. 这个映射正是所要求的逆函数. ■

设 $\varphi:S\longrightarrow T$ 是一个映射，并设 U 是 T 的子集合. U 的逆象定义为集合

【1.5】
$$\varphi^{-1}(U)=\{s\in S\mid \varphi(s)\in U\}.$$

无论 φ 是否有逆函数，这个集合都是有定义的. 这里的记号 φ^{-1} 只是作为符号使用.

一个集合称为有限的，如果它包含有限多个元素. 如果是这样的话，其元素的个数记为 $|S|$，有时称之为它的基数. 我们也把这个数称为 S 的阶. 如果 S 无限，记 $|S|=\infty$. 下面的定理是非常初等的，但它是一个非常重要的原理. 586

【1.6】定理　设 $\varphi:S\longrightarrow T$ 是有限集合间的映射.

(a) 如果 φ 是单的，则 $|S|\leqslant|T|$.

(b) 如果 φ 是满的，则 $|S|\geqslant|T|$

(c) 如果 $|S|=|T|$，则 φ 是一一的当且仅当它或是单的或是满的.

部分(a)的逆否命题常被称为鸽笼原理：如果 $|S|>|T|$，则 φ 不是单的. 例如，如果在 79 个抽屉里有 87 只袜子，则某个抽屉里至少有两只袜子.

一个无限集合 S 称为是可数的，如果存在一个从自然数集合到 S 的一一映射 $\varphi:\mathbb{N}\longrightarrow S$. 如果不存在这样的映射，则称 S 为不可数集.

【1.7】命题　实数集 $\mathbb{R}$ 是不可数集.

证明　这个证明常被称为康托尔的对角论证. 设 $\varphi:\mathbb{N}\longrightarrow\mathbb{R}$ 是任意映射. 我们将 φ 的象的元素按顺序 $\varphi(1)$，$\varphi(2)$，$\varphi(3)$，…列出，并将这些实数的每一个用十进制写出. 例如，列出的数的前面几个可能是：

$$\begin{array}{lcrl}
\varphi(1) & = & 8\ 2 & .\ \underline{3}\ 5\ 4\ 7\ 0\ 9\ 8\ 4\ 5\ 3\ 4\ \cdots \\
\varphi(2) & = & 0 & .\ 1\ \underline{2}\ 3\ 9\ 0\ 3\ 4\ 5\ 7\ 0\ 0\ \cdots \\
\varphi(3) & = & 5 & .\ 9\ 0\ \underline{8}\ 4\ 0\ 5\ 9\ 8\ 6\ 7\ 5\ \cdots \\
\varphi(4) & = & 1\ 2 & .\ 8\ 7\ 4\ \underline{3}\ 5\ 2\ 6\ 4\ 4\ 4\ 4\ \cdots \\
\varphi(5) & = & 0 & .\ 0\ 0\ 1\ 4\ \underline{4}\ 1\ 0\ 0\ 3\ 4\ 9\ \cdots \\
 & & & \qquad\quad \vdots
\end{array}$$

我们确定一个不在列表中的实数. 考虑其十进制展开由带下划线的数字组成的实数 u：$u=0.32834\cdots$. 通过改变这些数字中的每一个，我们构造一个新的实数，设为

$$v=0.45142\cdots.$$

注意因为 v 的第一位是 4，不等于 $\varphi(1)$ 的对应位上的数字 3，所以 $v\neq\varphi(1)$. 同样，因为 v 的

第二位是 5，不等于 $\varphi(2)$的对应位上的数字，所以 $v \neq \varphi(2)$. 类似地，对所有 n 有 $v \neq \varphi(n)$. 这表明 φ 不是满的，除了下面一点外，这就完成了证明.

有些实数有两个十进制展开：例如 0.99999…等于 1.00000…. 这给我们的论证带来一个问题. 必须选择 v 使其无限多位不等于 0 和 9. 最容易的办法是根本不选这两个数. ■

587 在本书中的一些地方我们提到了佐恩引理，它是一个处理无限集合的工具. 我们现在描述这个引理. 集合 S 上的一个偏序是一个在某些元素间成立的关系 $s \leqslant s'$，并且对 S 中所有的 s，s'，s''满足下列公理：

【1.8】

(i) $s \leqslant s$；

(ii) 如果 $s \leqslant s'$并且 $s' \leqslant s''$，则 $s \leqslant s''$；

(iii) 如果 $s \leqslant s'$并且 $s' \leqslant s$，则 $s = s'$.

一个偏序称为是一个全序，如果还有

(iv) 对 S 中所有的 s，s'有 $s \leqslant s'$或者 $s' \leqslant s$.

例如，设 S 是其元素为集合的集合. 如果 A，B 属于 S，我们可以定义 $A \leqslant B$，如果 $A \subset B$. 这是 S 上的一个偏序，称为按包含排序. 它是否是全序依赖于具体的情形.

如果 A 是偏序集 S 的子集，则 A 的一个上界是一个使得对所有 $a \in A$ 有 $a \leqslant b$ 的元素 $b \in S$. 偏序集 S 称为归纳的，如果 S 的每一个全序子集在 S 中有一个上界.

一个极大元素 $m \in S$ 是 S 中的没有比它更大的元素的元素，即除了 m 自己以外，不存在元素 $s \in S$ 使得 $m \leqslant s$. 这并不表明 m 是 S 的上界；特别地，可能存在许多互不相同的极大元素. 例如，$\{1, 2, \cdots, n\}$的所有真子集的集合包含 n 个极大元，其中之一是$\{1, 3, 4, \cdots, n\}$.

【1.9】引理 佐恩引理：一个归纳的偏序集有一个极大元.

佐恩引理等价于选择公理，后者已知是独立于集合论的基本公理的. 我们将不再进一步讨论这个等价关系，但将指出如何应用佐恩引理证明每个向量空间有一个基. 我们在这里使用向量的无序集.

【1.10】命题 域上每个向量空间 V 有一个基.

证明 取 V 的(无序)线性无关子集的集合为 S，像上面一样按包含排偏序. 我们验证 S 是归纳的：设 T 是 S 的一个全序子集. 则我们说组成 T 的集合的并也是线性无关的；因此它属于 S. 要验证这一点，令

$$B = \bigcup_{A \in T} A$$

是并集. 由定义，B 上的一个线性相关关系是有限的，因而可以写为

588 **【1.11】**

$$c_1 v_1 + \cdots + c_n v_n = 0$$

的形式，其中 $v_i \in B$. 由于 B 是集合 $A \in T$ 的并集，每个 v_i 包含在这些子集的一个中，称之为 A_i. 设 i，j 是两个下标. 由于 T 是全序的，$A_i \subset A_j$ 或 $A_j \subset A_i$. 由归纳法得到这些集合中的一个(比如说 A_i)包含所有其他的集合. 把这个集合记为 A. 则对所有 $i = 1, \cdots, n$ 有 $v_i \in A$. 由于 A 是线性无关的，因此(1.11)是平凡关系. 这表明 B 是线性无关的，因此是 S 的一个元素.

我们已经验证了佐恩引理的条件. 因而 S 包含一个极大元素 B. 我们断言 B 是一个基. 由

S 的定义，B 是线性无关的．设 $W=\mathrm{Span}(B)$．如果 $W<V$，则选择不属于 W 的元素 $v\in V$．于是集合 $B\cup\{v\}$ 是线性无关的[见第三章(3.10)]．这与 B 的极大性矛盾，并且说明 $W=V$，因此 B 是一个基． ■

类似的论证可以证明第十章的定理(8.3)．

【1.12】命题　设 R 是一个环．每个理想 $I\neq R$ 包含在一个极大理想中．

我们将证明留作练习．

第二节　证明技巧

数学家所认为的给出证明的适当的方法是没有明确定义的．通常并不是给出一个在每一步都由对上一步应用逻辑法则组成的意义下的完整的证明．写出这样一个证明会太长而且要点得不到突出．另一方面，证明中所有困难的步骤都认为应该包含在其中．读证明的人应该能够补充理解它所需的细节．如何写出证明是一种只有通过实践才能学会的技能．

我们将讨论用于构造证明的三个重要技巧：*二分法*、*归纳法*和*反证法*．

二分一词是指分成两部分．它用于把一个问题分解为更小、更易于处理的部分．这个过程的其他名称有*案例分析*和*分而治之*．这里是一个二分法的例子：二项式系数 $\binom{n}{k}$（读作 n 选 k）的定义为 $\binom{n}{k}$ 是在集合 $\{1, 2, \cdots, n\}$ 中 k 阶子集的个数．例如，$\binom{4}{2}=6$：$\{1, 2, 3, 4\}$ 的六个 2 阶子集是 $\{1, 2\}$，$\{1, 3\}$，$\{1, 4\}$，$\{2, 3\}$，$\{2, 4\}$，$\{3, 4\}$．

【2.1】命题　对每个整数 n 及每个 $k\leqslant n$，有 $\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}$．

证明　设 S 是 $\{1, 2, \cdots, n\}$ 的一个 k 阶子集．则或者 $n\in S$ 或者 $n\notin S$．这是我们的二分法．如果 $n\notin S$，则 S 实际上是 $\{1, 2, \cdots, n-1\}$ 的子集．由定义有 $\binom{n-1}{k}$ 个这样的子集．假设 $n\in S$，并设 $S'=S-\{n\}$ 是由从集合 S 删去元素 n 得到的子集．于是 S' 是 $\{1, 2, \cdots, n-1\}$ 的一个 $k-1$ 阶子集．有 $\binom{n-1}{k-1}$ 个这样的子集．因此有 $\binom{n-1}{k-1}$ 个 k 阶子集包含 n．这总共给出 $\binom{n-1}{k}+\binom{n-1}{k-1}$ 个 k 阶子集． ■

589

这里显示了二分法的巨大威力：在两种情形的每一种，即 $n\in S$ 和 $n\notin S$，我们都有一个关于集合 S 的另外的事实．这一另外的事实可以在证明中使用．

一个证明常常会需要整理出若干可能性，并逐个检查．这就是二分法或案例分析．例如要确定一个植物的种属，格雷的《植物学手册》提出一系列的二分法．一个典型例子是“叶子在茎上相对(见 h)，或叶子在茎上交错(见 k)”．数学结构的分类也要通过一系列的二分法来进行．在简单的情形中这不必正式地指出，但当处理复杂的可能性的范围时，就需要仔细地整理．下面是一个简单的例子：

【2.2】命题　每一个 4 阶群是阿贝尔群．

证明　设 G 是一个 4 阶群，并设 x，y 是 G 的两个元素．我们要证 $xy=yx$．考虑五个元

素 1，x，y，xy，yx. 由于群中只有四个元素，其中两个必相等. 如果 $xy=yx$，则命题已得到验证. 我们现在取遍其他情形：

情形 1：$x=1$ 或 $y=1$. 如果 $x=1$，则 $xy=y=yx$. 如果 $y=1$，则 $xy=x=yx$.

情形 2：$xy=1$ 或 $yx=1$. 于是 $y=x^{-1}$，且 $xy=1=yx$.

情形 3：$x=y$. 则 $xy=x^2=yx$.

情形 4：或者 $xy=x$，$yx=x$，$xy=y$，或者 $yx=y$. 在前两种情形，我们消去 x 得到 $y=1$，这回到情形 1. 后两种情形我们消去 y.

这耗尽了所有的可能性并完成了证明. ■

归纳法是证明一系列由正整数 n 作指标的命题 P_n 的主要方法. 为了对所有 n 证明命题 P_n，归纳法原理要求我们做两件事：

【2.3】

(i) 证明 P_1 成立；

(ii) 证明如果对某个整数 $k>1$ 有 P_k 成立，则 P_{k+1} 也成立.

有时证明如果对某个整数 $k\geqslant 0$，P_{k-1}成立，则 P_k 也成立更为方便. 这不过是指标变换.

下面是一些归纳法的例子.

【2.4】命题 上三角矩阵的行列式是其对角元素的乘积.

590

证明 这里 P_n 是断言命题对 $n\times n$ 三角矩阵成立. 在 1×1 矩阵的情形，只有一个对角元素，它等于行列式. 这意味着 P_1 成立. 我们现在假设 P_{k-1}成立，并用这个事实证明 P_k 成立. 设 A 是 $k\times k$ 三角矩阵. 我们按第一列的子式展开行列式：

$$\det A = a_{11}\det A_{11} - a_{21}\det A_{21} + \cdots.$$

由于 A 是三角矩阵，a_{21}，a_{31}，…，a_{k1}全都为零，因而 $\det A=a_{11}\det A_{11}$. 现在注意到 A_{11} 是一个$(k-1)\times(k-1)$三角矩阵且其对角元素为 a_{22}，a_{33}，…，a_{kk}. 由归纳假设 P_{k-1} 成立，因此 $\det A_{11}$ 是乘积 $a_{22}a_{33}\cdots a_{kk}$. 因而 $\det A=a_{11}a_{22}\cdots a_{kk}$，这正是要证的. ■

【2.5】命题 $\binom{n}{k}=\frac{n!}{k!\,(n-k)!}$.

证明 设 P_r 是断言：对 $k=1$，…，r 有 $\binom{r}{k}=\frac{r!}{k!\,(r-k)!}$. 假定 P_{r-1} 成立. 则当用 $n=r-1$和 $k=k$ 代入时公式成立，当用 $n=r-1$ 和 $k=k-1$ 代入时也成立：

$$\binom{r-1}{k}=\frac{(r-1)!}{k!(r-1-k)!},\quad \binom{r-1}{k-1}=\frac{(r-1)!}{(k-1)!(r-k)!}.$$

根据命题(2.1)，$\binom{r}{k}=\binom{r-1}{k}+\binom{r-1}{k-1}$. 这样

$$\binom{r}{k}=\binom{r-1}{k}+\binom{r-1}{k-1}=\frac{(r-1)!}{k!(r-1-k)!}+\frac{(r-1)!}{(k-1)!(r-k)!}$$

$$=\frac{(r-k)}{r}\frac{r!}{k!(r-k)!}+\frac{k}{r}\frac{r!}{k!(r-k)!}=\frac{r!}{k!(r-k)!}.$$

这表明 P_r 成立，这正是所要证的. ■

作为另一个例子，我们证明鸽笼原理(1.6a)，即如果有限集合间的一个映射 $\varphi: S \longrightarrow T$ 是单射，则 $|S| \leqslant |T|$. 我们对 $n=|T|$ 作归纳. 如果 $n=0$，即如果 T 是空集合，则断言是成立的，因为到空集合有映射的集合只能是空集合.

假设定理对 $n=k-1$ 已经证明，我们着手验证 $n=k$ 的情形，其中 $k>0$. 假设 $|T|=k$，且选择一个元素 $t\in T$.

情形 1：t 属于 φ 的象. 由于 φ 是单射，恰好存在一个元素 $s\in S$ 使得 $\varphi(s)=t$. 令 $S'=S-\{s\}$ 和 $T'=T-\{t\}$. 将 φ 限制到 S' 上，我们得到一个单射 φ': $S'\longrightarrow T'$. 由于 $|T'|=|T|-1=k-1$，我们的归纳假设表明 $|S'|\leqslant|T'|$. 因而 $|S|=|S'|+1\leqslant|T'|+1=|T|$.

情形 2：t 不属于 $\mathrm{im}\varphi$. 在这一情形 φ 的象包含在 $T'=T-\{t\}$ 中. 因而 φ 定义一个单射 $S\longrightarrow T'$. 我们的归纳假设再次表明 $|S|\leqslant|T'|=|T|-1$.

591

归纳法原理有一个变化，称为*完全归纳法*. 这里我们还是希望对每个正整数 n 证明断言 P_n. 完全归纳法原理断言只需证明如下断言：

【2.6】 *如果 n 是正整数，且如果对每个正整数 $k<n$，P_k 成立，则 P_n 成立.*

当 $n=1$ 时，没有满足 $k<n$ 的正整数. 因而对 $n=1$，(2.6)的假设自动地成立. 因此(2.6)的证明必包括 P_1 的证明.

当对某个较小的 k，有一个把 P_n 化为 P_k 而不一定是 P_{n-1} 的过程时，便使用完全归纳法原理. 下面是一个例子：

【2.7】定理 *每个整数 $n>1$ 是素整数的乘积.*

下面是一个非正式的证明，它亦展示了一个求素因数的算法：如果 n 是素整数，则它是一个素数的乘积，结论得证. 若不然，则它有一个异于 1 和 n 的因子. 如果 n 具体地给出，我们将能够检验是否有这样的真因子. 如果有，则 n 可以写成两个不是 1 的整数的乘积，比如 $n=ab$，且这时 a 和 b 都小于 n. 如果可能的话我们继续分解 a 和 b. 由于每次因数的大小减少，这一过程不能无限地继续，最后我们终止于 n 的一个素因子分解.

完全归纳法原理正式地陈述了不能无限次用更小的正整数替代一个正整数这种说法. 为应用这一原理，我们令 P_n 为 n 是素数的乘积这一断言，并且假设对所有 $k<n$ 有 P_k 成立. 我们再作一次论证. 要么 n 是素数，在这一情形我们的结论得证，否则 $n=ab$ 且 a 和 b 都小于 n. 在这种情形，归纳假设告诉我们 P_a 和 P_b 都成立，也就是说 a 和 b 都是素数的乘积. 把这两个积放在一起给出我们所要的 n 的因子分解.

两个证明看起来有点不同，因为算法在定理的陈述中没有被提到并且在正式的证明中受到忽视. 定理的一个更好的陈述应该显示出算法：

【2.8】定理 *分解一个 >1 的整数的过程在有限多步后终止.*

用这个陈述，正式证明和非正式证明是一致的.

*反证法*通过假设希望的结论是错的并由这个假设导出矛盾. 因而结论必是正确的. 例如我们可以这样重写上面给出的 4 阶群是阿贝尔群的证明：

592

(2.2)的证明(重写) 假设 G 是一个 4 阶非阿贝尔群，我们从这个假设导出矛盾. 由于 G

不是阿贝尔群，存在元素 x，$y\in G$ 使得 $xy\neq yx$. 则 y 不是元素 1，x，x^{-1} 中的任何一个，因为这些元素都与 x 交换. 类似地，x 不等于 1，y 或 y^{-1}. 我们现在可以验证元素 1，x，y，xy，yx 互不相同. 这与 $|G|=4$ 矛盾. 因而不存在 4 阶非阿贝尔群. ■

注意(2.2)的两个证明之间没有实际上的差别. 刚刚给出的证明实际上是伪反证法，虽然逻辑上没有问题，但在美学上不好接受. 应该避免用这样的方法写证明. 另一方面，有真正的反证法，这样的证明中不容易反过来消除矛盾. 书中给出的对一个素数 p，p^2 阶群是阿贝尔群[第六章(1.13)]的证明是一个例子，下面(3.11)给出的证明也是.

第三节 拓扑学

本节复习我们时常用到的拓扑学的概念. 我们想要研究的集合是欧几里得空间$\mathbb{R}^k$ 的子集.

设 r 是正实数. 关于点 $X\in\mathbb{R}^k$ 的半径为 r 的开球是到 X 的距离小于 r 的所有点的集合：

【3.1】
$$B_{X,r}=\{X'\in\mathbb{R}^k \mid |X'-X|<r\}.$$

$\mathbb{R}^k$ 的一个子集 U 称为开集，如果只要点 X 位于 U 中，则足够靠近 X 的点也在 U 中. 换言之，U 是开的，如果它满足下列条件：

【3.2】 如果 $X\in U$ 且如果 r 足够小，则 $B_{X,r}\subset U$.

半径 r 依赖于点 X.

开集具有下列性质：

【3.3】

(i) 任意开集簇的并是开集.

(ii) 有限多个开集的交是开集.

整个空间$\mathbb{R}^k$ 和空集合$\varnothing$是开集最简单的例子. 用下面的方法可得到一些更有意思的开集：设 f：$\mathbb{R}^k\longrightarrow\mathbb{R}$ 是连续函数. 则集合

593 **【3.4】** $\{f>0\}$，$\{f<0\}$，$\{f\neq 0\}$

是开集. 例如，如果 $f(X)>0$，则因为 f 连续，对所有 X 附近的 X'有 $f(X')>0$. 这表明一般线性群 $GL_2(\mathbb{R})$是所有 2×2 矩阵空间$\mathbb{R}^4$ 的一个开子集，这是因为它是集合$\{\det P\neq 0\}$. 此外，开球 $B_{X,r}$是$\mathbb{R}^k$ 中的一个开集，因为它是由不等式 $|X'-X|-r<0$ 定义的.

设 S 是$\mathbb{R}^k$ 的任意子集. 我们还需要 S 的开子集的概念. 由定义，S 的一个子集 V 称为在 S 中是开的，如果只要它包含 S 中一个点 X，则它也包含 S 中所有充分靠近 X 的点. 下面的引理解释了这个条件：

【3.5】引理 *设 V 是$\mathbb{R}^k$ 的集合 S 的一个子集. 在 V 上下列条件等价. 如果其中之一成立，则 V 称为 S 的开子集：*

(i) 对$\mathbb{R}^k$ 的某个开集 U 有 $V=U\cap S$.

(ii) 对每个点 $X\in V$，存在 $r>0$ 使得 V 包含集合 $B_{X,r}\cap S$.

证明 假设对$\mathbb{R}^k$ 的某个开集 U 有 $V=U\cap S$. 设 $X\in V$. 则 $X\in U$，且(3.2)保证存在一个 $r>0$ 使得 $B_{X,r}\subset U$. 因而 $B_{X,r}\cap S\subset U\cap S=V$，这就验证了(ii). 反之，假定(ii)成立. 对每个

$X\in V$，选择一个开球 $B_{X,r}$ 使得 $B_{X,r}\cap S\subset V$，像通常一样半径 r 依赖于点 X. 设 U 是这些球的并集. 则 U 是$\mathbb{R}^k$ 的开集(3.3i)，并且 $U\cap S\subset V$. 另一方面，对每个 $X\in V$ 有 $X\in B_{X,r}\cap S\subset U\cap S$. 因而 $V\subset U\cap S$，因而 $V=U\cap S$，这正是要证明的. ■

S 的开子集具有性质(3.3)，因为(3.5i)，这由$\mathbb{R}^k$ 的开子集同样的性质得到.

习惯上把包含一个给定点 p 的 S 的开子集 V 称为 p 在 S 中的一个邻域.

集合 S 的子集 C 称为闭的，如果其补集$(S-C)$是开的. 例如，设 f_i：$\mathbb{R}^k\longrightarrow\mathbb{R}$ $(i=1,\cdots,k)$ 是连续函数. 则 k 个方程 $f_i=0$ 的解的轨迹

【3.6】 $$\{f_1=f_2=\cdots=f_k=0\}$$

是$\mathbb{R}^k$ 的闭集，因为它的补集是开集$\{f_i\neq 0\}$的并. 2-球面$\{x_1^2+x_2^2+x_3^2=1\}$是$\mathbb{R}^3$ 的闭集的例子. 旋转群 SO_2 也是. 它是$\mathbb{R}^{2\times 2}$中由五个方程

$$x_{11}x_{22}-x_{12}x_{21}=1,\quad x_{11}^2+x_{12}x_{21}=1,\quad x_{21}x_{12}+x_{22}^2=1,$$
$$x_{11}x_{12}+x_{12}x_{22}=0,\quad x_{21}x_{11}+x_{22}x_{21}=0$$

定义的轨迹.

闭集有与(3.3)对偶的性质：

【3.7】

(i) 任意闭集簇的交是闭的.

(ii) 有限多个闭集的并是闭的.

这些规则由(3.3)取补得到.

$\mathbb{R}^k$ 的子集 C 称为有界的，如果 C 中点的坐标是有界的，就是说存在一个界，即一个正实数 b 使得对 $X=(x_1,\cdots,x_n)\in C$ 及所有 $i=1,\cdots,n$，有

【3.8】 $$|x_i|\leqslant b.$$

如果 C 同时是闭的和有界的，则称之为$\mathbb{R}^k$ 的一个紧子集. 单位 2-球面是$\mathbb{R}^3$ 的一个紧子集.

设 S，T 是$\mathbb{R}^m$ 和$\mathbb{R}^n$ 的子集. 一个映射 f：$S\longrightarrow T$ 称为连续的，如果它将 S 中邻近的点变为 T 的邻近的点. 连续性正式的表述为：

【3.9】 *设 $s\in S$. 对每个实数 $\varepsilon>0$，存在一个 $\delta>0$ 使得如果 $s'\in S$ 且 $|s'-s|<\delta$，则 $|f(s')-f(s)|<\varepsilon$.*

得到从 S 到 T 的连续映射的最简单的办法是取恰好把 S 映到 T 的连续映射 F：$\mathbb{R}^m\longrightarrow\mathbb{R}^n$ 的限制. 我们用到的大多数映射都是这个类型. 例如，行列式是从任一个典型群到$\mathbb{R}$ 或$\mathbb{C}$ 的连续函数.

一个映射 f：$S\longrightarrow S'$称为一个同胚，如果它是一一的且 f^{-1} 以及 f 都是连续的.

例如，$\mathbb{R}^2$ 中的单位圆 S^1 与旋转群 SO_2 同胚. 同胚 f：$S^1\longrightarrow SO_2$ 通过将$\mathbb{R}^2$ 映到 2×2 矩阵空间$\mathbb{R}^4$ 的映射

$$F(x_1,x_2)=\begin{bmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{bmatrix}$$

进行限制给出. 映射 F 不是一一的，因而不是同胚，但它限制到子集 S^1 和 SO_2 上的一个同胚 f. 其逆是将 2×2 矩阵映到其顶行的投射 G：$\mathbb{R}^4\to\mathbb{R}^2$ 在 SO_2 的限制. (同胚一词不能与同态混淆!)

一条路是由单位区间到空间$\mathbb{R}^k$的一个连续映射f：$[0, 1] \longrightarrow \mathbb{R}^k$，并称这条路位于$S$中，如果对每个$t \in [0, 1]$，有$f(t) \in S$. $\mathbb{R}^k$的一个子集S称为路连通的，如果每对点p，$q \in S$可由位于S中的路连接起来．换言之，对每对点p，$q \in S$，存在一条路f使得

【3.10】

(i) 对区间中的每个t有$f(t) \in S$.

(ii) $f(0)=p$及$f(1)=q$.

下面是路连通集合最重要的性质：

【3.11】命题 路连通集合S不是真的开子集的不相交并．换言之，假设

595

$$S = \bigcup_{\alpha} V_i,$$

其中V_i是S的开子集且对$i \neq j$有$V_i \cap V_j = \varnothing$．则集合$V_i$中除了一个外都是空的．

证明 假设集合中有两个非空，如设为V_0和V_1．我们取定V_0并用剩下子集的并替代V_1，由(3.3)，它是开集．于是$V_0 \cup V_1 = S$且$V_0 \cap V_1 = \varnothing$．这化为恰好有两个开集的情形．

选择点$p \in V_0$和$q \in V_1$，并设f：$[0, 1] \longrightarrow S$是S中连接p到q的一条路．通过检查路最后一次离开V_0的点我们将得到一个矛盾．

设b是使得$f(t) \in V_0$的$t \in [0, 1]$的最小上界，并设$X=f(b)$．如果$X \in V_0$，则如果r足够小，$B_{X,r} \cap S$的所有点属于V_0．由于f连续，对所有充分靠近b的点t有$f(t) \in B_{X,r}$．因而对这些点有$f(t) \in V_0$．取一个比b稍大的元素而产生与b作为映到V_0中元素的上界的矛盾．因而X不属于V_0，这样它必属于V_1．但以同样的方式推理，我们得到对所有充分靠近b的t有$f(t) \in V_1$．取一个比b稍小的元素t而产生与b作为映到V_0中元素的最小上界的矛盾．这一矛盾完成了证明． ■

最后一个来自拓扑的概念是流形．

【3.12】定义 $\mathbb{R}^n$的一个子集S称为d维流形，如果S的每个点p有一个与$\mathbb{R}^d$的一个开集同胚的邻域．

例如，球面$\{(x, y, z) \mid x^2+y^2+z^2=1\}$是一个二维流形．半球面$U=\{z>0\}$是$S^3$中的开集(3.4，3.5)且连续地投射到$\mathbb{R}^3$的单位球$B_{0,1}=\{x_1^2+x_2^2+x_3^2<1\}$．逆函数$z=\sqrt{1-x^2-y^2}$是连续的．因而$U$与$B_{0,1}$同胚．由于3-球面是被这样的半球所覆盖的，因而它是一个流形．

下图所示的是一个非流形的集合．当把点p删去时它成为一个1维流形．注意对这个集合没有齐性．它在p点附近和其他点附近看起来不一样．

【3.13】图

p

596

不是流形的集合

第四节 隐函数定理

本书中两处用到了隐函数定理，我们把它叙述在这里作为参考.

【4.1】定理 隐函数定理：设 $f(x, y)=(f_1(x, y), \cdots, f_r(x, y))$ 是 $n+r$ 个实变量 $(x, y)=(x_1, \cdots, x_m, y_1, \cdots, y_r)$ 的函数，它在 $\mathbb{R}^{n+r}$ 中包含点 (a, b) 的一个开集上有连续偏导数. 假设雅可比行列式

$$\det\begin{bmatrix}\frac{\partial f_1}{\partial y_1} & \cdots & \frac{\partial f_1}{\partial y_r}\\ \vdots & & \vdots\\ \frac{\partial f_r}{\partial y_1} & \cdots & \frac{\partial f_r}{\partial y_r}\end{bmatrix}$$

在点 (a, b) 不为零. 存在点 a 在 $\mathbb{R}^n$ 中的邻域 U，使得存在 U 上唯一的连续可微函数 $Y_1(x), \cdots, Y_r(x)$ 满足条件

$$f(x,Y(x))=0 \quad 且 \quad Y(a)=b.$$

隐函数定理与第八章(5.8)用到的逆函数定理有着密切的联系：

【4.2】定理 逆函数定理：设 f 是从 $\mathbb{R}^n$ 的开集 U 到 $\mathbb{R}^n$ 的连续可微映射. 假设雅可比行列式

$$\det\begin{bmatrix}\frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n}\\ \vdots & & \vdots\\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n}\end{bmatrix}$$

在点 $a\in\mathbb{R}^n$ 不等于零. 则存在 a 的一个邻域，在它上面 f 有连续可微的逆函数.

这两个定理的证明请参考在“进一步阅读建议”中所列的卢丁(Rudin)的书中.

我们还在一个地方[第十三章(8.14)]用到了下面的隐函数定理的一个复的类似：

【4.3】定理 设 $f(x, y)$ 为一个复多项式. 假设对某个 $(a, b)\in\mathbb{C}^2$，我们有 $f(a, b)=0$ 且 $\frac{\partial f}{\partial y}(a, b)\neq 0$. 存在 x 在 $\mathbb{C}$ 中的一个邻域 U，在这个邻域上面存在一个唯一的连续函数 $Y(x)$，它具有下列性质：

$$f(x,Y(x))=0, \quad Y(a)=b.$$

由于对这个拓广的参考文献不太常见，我们将给出一个把它化为实隐函数定理的证明. 方法是简单地把所有的东西都用它们的实部和虚部表出，然后验证(4.1)的假设. 同样的论证对更多的变量也可应用.

证明 记 $x=x_0+\mathrm{i}x_1$，$y=y_0+\mathrm{i}y_1$，$f=f_0+\mathrm{i}f_1$，其中 $f_i=f_i(x_0, x_1, y_0, y_1)$ 是四个实变量的实值函数. 我们要对 y_0，y_1 作为 x_0，x_1 的函数解一对方程 $f_0=f_1=0$. 根据(4.1)，我们要证明在 (a, b) 雅可比行列式

$$\det\begin{bmatrix}\dfrac{\partial f_0}{\partial y_0} & \dfrac{\partial f_0}{\partial y_1}\\ \dfrac{\partial f_1}{\partial y_0} & \dfrac{\partial f_1}{\partial y_1}\end{bmatrix}$$

不为零．因为 f 是 x，y 的多项式，实函数 f_i 也是 x_i，y_i 的多项式．因而它们有连续的导数．

【4.4】引理 设 $f(x, y)$ 为一个复系数多项式．用上面的记号，有

(i) $\dfrac{\partial f}{\partial y}=\dfrac{\partial f_0}{\partial y_0}+\dfrac{\partial f_1}{\partial y_0}\mathrm{i}$，

(ii) 柯西-黎曼方程 $\dfrac{\partial f_0}{\partial y_0}=\dfrac{\partial f_1}{\partial y_1}$ 和 $\dfrac{\partial f_0}{\partial y_1}=-\dfrac{\partial f_1}{\partial y_0}$ 成立．

引理的证明 由于 f 是多项式并且由于和的导数是导数的和，因此只要对单项式 $cy^n=(c_0+c_1\mathrm{i})(y_0+y_1\mathrm{i})^n$ 证明引理就行了．对这些单项式，引理由微分乘法法则对 n 作归纳得到．■

我们回到定理(4.3)的证明．由假设，$f_i(a_0, a_1, b_0, b_1)=0$．同样，由于 $\dfrac{\partial f}{\partial y}(a, b)\neq 0$，由(4.4i)可知 $\dfrac{\partial f_0}{\partial y_0}=d_0$ 和 $\dfrac{\partial f_1}{\partial y_0}=d_1$ 不同时为零．由(4.4ii)，雅可比行列式为

$$\det\begin{bmatrix}d_0 & -d_1\\ d_1 & d_0\end{bmatrix}=d_0^2+d_1^2>0.$$

598 这表明满足隐函数定理(4.1)的假设．■

练　　习

第一节　集合论

1. 设 φ: Z ⟶ R 是由 $\varphi(n)=n^3-3n+1$ 定义的映射．
   (a) φ 是单射吗？
   (b) 求 $\varphi^{-1}(U)$，其中 U 是区间(i)$[0, \infty)$，(ii)$[2, 4]$，(iii)$[4, 12]$．
2. 举出一个无限集到自身的映射 $\varphi: S\longrightarrow S$ 是满射而不是单射的例子和一个是单射而不是满射的例子．
3. 设 $\varphi: S\longrightarrow T$ 是集合的映射．
   (a) 设 U 是 S 的子集．证明 $\varphi(\varphi^{-1}(U))\subset U$，且如果 φ 是满射，则 $\varphi(\varphi^{-1}(U))=U$．
   (b) 设 V 是 T 的子集．证明 $\varphi^{-1}(\varphi(V))\supset V$，且如果 φ 是单射，则 $\varphi^{-1}(\varphi(V))=V$．
4. 设 $\varphi: S\longrightarrow T$ 是非空集合的映射．一个映射 ψ: $T\longrightarrow S$ 是一个*左逆*，如果 $\psi\circ\varphi: S\longrightarrow S$ 是恒等映射，而它是一个*右逆*，如果 $\varphi\circ\psi$: $T\longrightarrow T$ 是恒等映射．证明 φ 有左逆当且仅当它是单射而它有右逆当且仅当它是满射．
5. 设 S 是一个偏序集．
   (a) 证明如果 S 包含 S 的一个上界 b，则 b 是唯一的，并且 b 还是一个极大元．
   (b) 证明如果 S 是全序的，则极大元 m 是 S 的一个上界．
6. (a) 精确描述哪些实数有多于一个十进制展开式以及这样一个实数有多少个展开式．
   (b) 修正命题(1.7)的证明．
7. 用佐恩引理证明每个理想 $I\neq R$ 包含在一个极大理想中．通过证明所有理想 $I\neq R$ 的集合 S(以包含排序)是一个归纳集．

第二节 证明技巧

1. 用归纳法求下列表达式的一个紧凑型形式.

 (a) $1+3+5+\cdots+(2n+1)$

 (b) $1^2+2^2+3^2+\cdots+n^2$

 (c) $1+1/2+1/3+\cdots+1/n$

 (d) $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n(n+1)}$

2. 证明 $1^3+2^3+\cdots+n^3=(n(n+1))^2/4$.

3. 证明 $1/(1\cdot 2)+1/(2\cdot 3)+\cdots+1/(n(n+1))=n/(n+1)$.

4. 设 S, T 是有限集.

 (a) 令 $\varphi: S\longrightarrow T$ 是一个单映射. 归纳证明 $|S|\leqslant|T|$ 且如果 $|S|=|T|$, 则 φ 是一一映射.

 (b) 令 $\varphi: S\longrightarrow T$ 是一个满映射. 归纳证明 $|S|\geqslant|T|$ 且如果 $|S|=|T|$, 则 φ 是一一映射.

5. 设 n 是一个正整数. 证明如果 2^n-1 是素数, 则 n 是素数.

6. 设 $a_n=2^{2^n}+1$. 证明 $a_n=a_0a_1\cdots a_{n-1}+2$.

7. 有理系数多项式称为既约的, 如果它不是常数并且它不是两个非常数有理系数多项式的乘积. 用完全归纳法证明每个有理系数多项式可以写为既约多项式的乘积.

8. 证明定理(1.6)的(b)和(c).

599

第三节 拓扑学

1. 设 S 是$\mathbb{R}^k$ 的一个子集, 并设 f, g 是 S 到$\mathbb{R}$的连续映射. 确定下列子集在 S 中是否开或闭.

 (a) $\{f(X)\geqslant 0\}$ (b) $\{f(X)\neq 2\}$ (c) $\{f(X)<0, g(X)>0\}$ (d) $\{f(X)\leqslant 0, g(X)<0\}$

 (e) $\{f(X)\neq 0, g(X)=0\}$ (f) $\{f(X)\in\mathbb{Z}\}$ (g) $\{f(X)\in\mathbb{Q}\}$

2. 设 $X\in\mathbb{R}^n$. 确定下列集合是否开或闭.

 (a) $\{rX \mid r\in\mathbb{R}, r>0\}$ (b) $\{rX \mid r\in\mathbb{R}, r\geqslant 0\}$

3. (a) 设 $P=(p_{ij})$是一个可逆矩阵, 并设 $d=\det P$. 我们可以通过使 $P\rightsquigarrow(p_{ij}, d)$定义一个映射 $GL_n(\mathbb{R})\longrightarrow\mathbb{R}^{n^2+1}$. 证明这一法则将 $GL_n(\mathbb{R})$作为闭集嵌入$\mathbb{R}^{n^2+1}$.

 (b) 在 $GL_1(\mathbb{R})$的情形描述这个映射.

4. 证明两个流形 M, M'的积 $M\times M'$是一个流形.

5. 证明 $SL_2(\mathbb{R})$不是一个紧群.

6. (a) 作出$\mathbb{R}^2$ 中的曲线 C: $x_2^2=x_1^3-x_1^2$ 的略图.

 (b) 证明如果删去原点, 这个轨迹是一维流形.

第四节 隐函数定理

1. 证明引理(4.4).

2. 证明 $SL_2(\mathbb{R})$是流形, 并求其维数.

3. 设 $f(x, y)$是复多项式, 假设方程

$$f=0,\quad \frac{\partial f}{\partial x}=0,\quad \frac{\partial f}{\partial y}=0$$

在$\mathbb{C}^2$ 中没有公共解. 证明 $f=0$ 的轨迹是一个 2 维流形.

600

记　号

A_n	交错群，第二章(4.7)
$B_{X,r}$	关于点 X 半径为 r 的开球，附录(3.1)
$\mathbb{C}$	复数域，第二章(1.11)
C_n	n 阶循环群，第五章(3.4)
D_n	二面体群，第五章(3.4)
det	行列式，第一章(3.4)
$\mathbb{F}_p$	素域 $\mathbb{Z}/(p)$，第三章(2.4)
GL_n	一般线性群，第二章(1.13)
I	单位矩阵，第一章(1.14)
I	二十面体群，第五章(9.1)
$\mathrm{im}\varphi$	映射 φ 的象，附录(1.3)
$\ker\varphi$	同态 φ 的核，第二章(4.5)
ℓ^∞	有界序列空间，第三章(5.2)
M	平面运动群，第四章(5.15)，第五章(2.1)
$N(H)$	H 的正规化子，第六章(3.7)
$\mathbb{N}$	正整数集合或自然数，第十章(2.1)
O_n	正交群，第五章(5.3)，第八章(1.3)
$O_{3,1}$	洛伦兹群，第八章(1.4)
PSL_n	射影群，第八章(8.2)
$\mathbb{R}$	实数域，第二章(1.11)
$\mathbb{R}^n$	n-维向量空间，第三章(1.1)
S_n	对称群，第二章(1.14)
S^n	n-球面，第八章(2.6)
SL_n	特殊线性群，第二章(4.6)，第八章(1.8)
SO_n	特殊正交群，第四章(5.4)，第八章(1.8)
SP_{2n}	辛群，第八章(1.6)
SU_n	特殊酉群，第八章(1.8)
T	正四面体群，第五章(9.1)
^{t}	(上标 t)矩阵的转置，第一章(2.24)
tr	迹，第四章(4.18)
U_n	酉群，第七章(4.15)，第八章(1.8)
Z	群的中心，第二章(4.10)
$\mathbb{Z}$	整数环，第二章(1.11)

$Z(x)$	x 的中心化子，第六章(1.5)
$*$	如果 A 是复矩阵，则 $A^*=\overline{A}^t$，第七章(4.7)
	在矩阵的表示中，$*$ 表示未定元素，第一章(1.15)
	带星号的练习是较难的
$^+$	(上标＋)合成法则为加法的群，第二章(1.1)
$^\times$	(上标×)合成法则为乘法的群，第二章(1.1)
$\oplus$	直和，第三章(6.4)，第十二章(6.3)
!	阶乘 $n!$，即整数 1，2，…，n 的乘积
$\binom{n}{k}$	二项式系数，附录(2.1)
$[\mu]$	$\leqslant\mu$ 的最大整数，第十一章(10.23)

601

如果 S 和 T 为集合，有如下记号：

$\lvert S\rvert$	元素的个数，也称为集合 S 的阶
$s\in S$	s 是 S 的一个元素
$S\subset T$	S 是 T 的子集，或 S 包含在 T 中．换言之，S 的每个元素也是 T 的元素
$T\supset S$	T 包含 S，这与 $S\subset T$ 是一回事
$S<T$	S 是 T 的真子集，意指它是子集，且 T 含有不是 S 的成员的元素
$T>S$	这与 $S<T$ 是一回事
$T-S$	只有当 S 是 T 的子集时才使用，它表示 S 在 T 中的补集，即所有属于 T 但不属于 S 的集合：$T-S=\{x \mid x\in T \text{但} x\notin S\}$
$S\cap T$	集合 S 和 T 的交，它是 S 和 T 所有公共元素的集合
$S\cup T$	集合 S 和 T 的并，它是包含在集合 S 和 T 之一中的元素 x 的集合
$S\times T$	集合的积．其元素是元素的有序对(s,t)：$S\times T=\{(s,t) \mid s\in S, t\in T\}$ 由于括号有其他意义，我们有时将其省去，将积集的元素记为 s，t
$\varphi:S\longrightarrow T$	从 S 到 T 的一个映射，或其定义域为 S 而值域为 T 的一个函数
$s \rightsquigarrow t$	箭头指出所讨论的映射将把元素 s 映为元素 t，即 $\varphi(s)=t$
■	文中话题的转移，如证明结束了，回到主线

602

进一步阅读建议

一般代数教材：

G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, 3rd ed., Macmillian, New York, 1965.

I. N. Herstein, *Topics in Algebra*, 2nd ed., Wiley, New York, 1975.

N. Jacobson, *Basic Algebra I, II*, Freeman, San Francisco, 1974, 1980.

S. Lang, *Algebra*, 2nd ed, Addison-Wesley, Reading, MA, 1965.

H. Paley and P. M. Weichsel, *Elements of Abstract and Linear Algebra*, Holt, Reinhart and Winston, New York, 1972.

B. L. van der Waerden, *Modern Algebra*, Ungar, New York, 1970.

数学史：

N. Bourbaki, *Eléments d'histoire des mathématiques*, Hermann, Paris, 1974.

H. Edwards, *Fermat's Last Theorem*, Springer-Verlag, New York, 1977.

H. Edwards, *Galois Theory*, Springer-Verlag, New York, 1984.

Morris Klein, *Mathematical Thought from Ancient to Modern Times*, Oxford, New York, 1972.

B. L. van der Waerden, *A History of Algebra*, Springer-Verlag, Berlin, New York, 1985.

第一章：

603

T. Muir, *A Treatise on the Theory of Determinants*, Dover, New York, 1960.

第二章：

I. N. Herstein, *Topics in Algebra*, 2nd ed, Wiley, New York, 1975.

第三、四章：

G. Strang, *Linear Algebra and Its Applications*, 3rd ed., Harcourt Brace Jovanovich, San Diego, 1988.

第五章：

C. T. Benson and L. C. Grove, *Finite Reflection Groups*, 2nd ed., Springer-Verlag, New York, 1985.

H. M. S. Coxeter, *Introduction to Geometry*, Wiley, New York, 1961.

L. Ford, *Automorphic Functions*, Chelsea, New York, 1929.

B. Grünbaum and G. C. Sheppard, *Tilings and Patterns*, W. H. Freeman, New York, 1967.

H. W. Guggenheimer, *Plane Geometry and Its Groups*, Holden-Day, San Francisco, 1967.

第七章：

B. Noble，*Applied Linear Algebra*，2nd ed.，Prentice Hall，Englewood Cliffs，NJ，1977.

第八章：

R. Howe，"Very Basic Lie Theory,"*Math Monthly* 90(1983)600-623.

F. Warner，*Foundations of Differential Geometry and Lie Groups*，Springer-Verlag，New York，1983.

H. Weyl，*The Classical Groups*，Princeton University Press，Princeton，1946.

第九章：

J.-P. Serre，*Linear Representations of Finite Groups*，Springer-Verlag，New York，1977.

第十章：

K. Kendig，*Elementary Algebraic Geometry*，Springer-Verlag，New York，1976.

E. Landau，*Foundations of Analysis*，Chelsea，New York，1960. [604]

第十一章：

Z. I. Borevich and I. R. Shafarevitch，*Number Theory*，Academic Press，New York，1966.

H. Edwards，*Fermat's Last Theorem*，Springer-Verlag，New York，1977.

K. F. Gauss，*Disquisitiones Arithmeticae*，Leipzig，1801.

H. Hasse，*Number Theory*，Springer-Verlag，New York，1980.

J.-P. Serre，*A Course in Arithmetic*，Springer-Verlag，New York，1973.

H. Stark，*An Introduction to Number Theory*，M. I. T. Press，Cambridge，1978.

第十三章：

G. A. Bliss，*Algebraic Functions*，AMS Colloquium Publications No. XVI，New York，1933.

第十四章：

H. Edwards，*Galois Theory*，Springer-Verlag，New York，1984.

附录：

J. R. Munkres，*Topology：A First Course*，Prentice Hall，Englewood Cliffs，NJ，1975.

W. Rudin，*Principles of Mathematical Analysis*，3rd ed.，McGraw-Hill，New York，1976. [605]

索 引

索引中的页码为英文原书页码，与书中页边标注的页码一致．

D

G

J

K

L

M

P

T

U

V

华章数学译丛

数学文化
数学简史（Katz，英）

微积分
高等微积分（Fitzpatrick，中、英）
微积分及其应用（Bittinger，中）
托马斯大学微积分（Hass，中）

数学分析
数学分析原理（Rudin，中、英）
数学分析（Apostol，中、英）
纯数学教程（Hardy，英）
泛函分析（Rudin，中、英）
实分析与复分析（Rudin，中、英）
实分析（Royden，中、英）
实分析和概率论（Dudley，中、英）
复分析（Ahlfors，中、英）
复变函数及应用（Brown，中、英）
复分析基础及工程应用（Saff，中、英）
三角级数（Zygmund，英）

调和分析
调和分析导论（Katznelson，英）
逼近论教程（Cheney，英）
小波基础及应用教程（Mix，中）
小波与小波变换导论（Burrus，中、英）
小波分析及其应用（孙延奎，编写）
傅里叶分析与小波分析导论（Pinsky，英）
时频变换与小波变换导论（钱世锷，英）

代数
线性代数（Jain，英）
线性代数（Leon，中、英）
线性代数及其应用（Lay，中）
代数（Isaacs，英）
代数（Artin，中、英）
抽象代数基础教程（Rotman，中、英）
高等近世代数（Rotman，中）
矩阵分析（Horn，中）
同调代数导论（Weibel，英）

几何、拓扑
曲线与曲面的微分几何（do Carmo，中、英）
微分几何及其应用（Oprea，中、英）
分形分析（Kigami，英）
拓扑学（Munkres，中、英）

数学建模
数学建模方法与分析（Meerschaert，中）
数学建模（Giordano，中、英）

微分方程
实用偏微分方程（Haberman，中、英）
偏微分方程教程（Asmar，中、英）
微分方程与边界值问题（Zill，中、英）
动力系统导论（Robinson，中、英）
流体动力学导论（Batchelor，英）

计算数学
数值方法和MATLAB实现与应用（Recktenwald，中）
数值分析（Kincaid，中、英）
数值方法（金一庆，编写）
计算机数值计算方法及程序设计（周煦，编写）
科学计算导论：使用MATLAB的矩阵向量方法（Van Loan，英）
MATLAB数值计算（Moler，中）
具体数学：计算机科学基础（Graham，中、英）

概率统计
概率论与数理统计（陈方樱，编写）
概率论基础教程（Ross，中）
概率统计（Stone，英）

华章数学译丛

概率论及其在投资、保险、工程中的应用（Bean，英）
概率与计算（Mitzenmacher，中）
贝叶斯方法（Leonard，英）
抽样理论与方法（Govindarajulu，英）
数理统计与数据分析（Rice，英）
应用回归分析和其他多元方法（Kleinbaum，英）
多元数据分析（Lattin，英）
预测与时间序列（Bowerman，英）
时间序列分析的小波方法（Percival，中、英）
随机过程导论（Kao，英）
试验者的统计学（Box，中）
理工科概率统计（Walpole，中）
统计学（Mendenhall，中）

离散数学

离散数学（陈国勋，编写）
离散数学导学（Simpson，中）
离散数学及其应用（Rosen，中、英）
离散数学（Dossey，中、英）
离散数学及其应用（徐凤生，编写）

组合数学

组合数学教程（van Lint，中、英）
组合数学（Brualdi，中、英）
应用组合数学（Roberts，中、英）
计数组合学：卷1、卷2（Stanley，英）
图论导引（West，中、英）
图论（Tutte，英）
网络流：理论、算法与应用（Ahuja，英）

数论

初等数论及其应用（Rosen，中、英）
数论概论（Silverman，中、英）

数理逻辑

应用逻辑（Nerode，中、英）

金融数学

金融数学（Stampfli，中、英）
数理金融初步（Ross，中、英）
金融时间序列分析（Tsay，中）

运筹学

数学规划导论（Walker，英）
线性规划导论（Vaserstein，中、英）

数学软件

LATEX实用教程（Kopka，英）
MATLAB 7及工程问题解决方案（Etter，中）
SAS统计分析及应用（黄燕，编写）